Délibération n°89/2005 du 21 décembre 2005 de la Commission nationale pour la protection des données relative à la demande d'autorisation préalable introduite par l'établissement public Domaine Thermal de Mondorf en matière de traitement à des fins de surveillance contenant des données biométriques.

I. Procédure et forme de la demande

L'établissement public de droit luxembourgeois Domaine Thermal de Mondorf (ci-après désigné « le requérant »), établi et ayant son siège à L-5601 Mondorf-les-Bains, Avenue des Bains, a introduit par requête du 31 octobre 2005, une demande d'autorisation, enregistrée sous les références R002245 / A002062, sur base de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après en abrégé « la loi »).

La Commission nationale pour la protection des données (ci-après « la Commission nationale ») constate que le requérant s'est désigné lui-même comme responsable du traitement, en indiquant comme son représentant Monsieur Marc OLINGER, Directeur.

- Compétence

La Commission nationale se déclare compétente pour examiner la demande d'autorisation sur base des articles 3, 10, 14 paragraphe (1) lettre (a), 32 paragraphe (3) lettre (d) et 33 paragraphe (1) lettre (c) de la loi.

- Recevabilité

La demande d'autorisation est recevable, étant donné que celle-ci contient toutes les informations obligatoires mentionnées à l'article 14 paragraphe (2) de la loi.

- Quant aux formalités préalables à l'autorisation de traitement prescrites par la loi

La Commission nationale relève que l'article 14 de la loi exige que les demandes d'autorisation doivent être préalables à la mise en œuvre du traitement envisagé. Son paragraphe (4) prévoit d'ailleurs que, dans le cas contraire, le contrevenant s'expose à des peines correctionnelles.

En l'espèce, le requérant a déposé sa demande d'autorisation le 31 octobre 2005 alors que le traitement a été mis en oeuvre depuis le 21 septembre 2005.

Dans son courrier du 23 septembre 2005, la Commission nationale avait rendu le requérant attentif à ce problème et avait exigé la cessation immédiate du traitement en question jusqu'à ce qu'elle se prononce formellement sur le traitement mis en place.

Il convient de préciser que dès la mise en place du traitement un certain nombre d'abonnés s'étaient plaints auprès de la Commission nationale parce que les agents du Centre thermal menaçaient de leur interdire l'accès aux installations en tant qu'abonnés dès lors qu'ils refuseraient de se prêter à la collecte de leurs empreintes digitales et d'utiliser à l'avenir le système en question lors de leur accès aux installations ; le requérant leur proposait alors le remboursement du solde de l'abonnement.

Dans un courrier du 28 septembre 2005, la Commission nationale informait la direction du Domaine Thermal qu'elle ne saurait accepter que ces personnes subissent un traitement désavantageux au niveau des conditions financières et des modalités pratiques de l'accès aux installations et ce aussi longtemps que la Commission nationale n'aurait pas statué sur la demande d'autorisation. Dans l'attente de prendre position sur le traitement envisagé, la Commission a exigé que le requérant propose des mesures alternatives pour les abonnés qui refusent de donner leurs empreintes digitales. Les responsable du Centre thermal avaient alors répondu que ces personnes pourraient continuer à utiliser leur abonnement sans devoir fournir leurs empreintes digitales, qu'elles seraient conduites à l'accueil par un préposé pour accéder aux installations et qu'elles n'avaient pas non plus à subir un quelconque délai d'attente.

Or, il semblerait qu'aujourd'hui le requérant ne propose plus cette alternative : les abonnés qui refusent de donner leurs empreintes digitales reçoivent des tickets, à l'instar des visiteurs journaliers, de sorte qu'ils subissent les délais d'attente. La Commission nationale regrette que le Centre thermal n'ait pas respecté ses recommandations.

II. <u>Objet de la demande et bien-fondé</u>

- **Description du traitement envisagé**

Depuis le 21 septembre 2005, le requérant a mis en place un système d'accès à ses installations réservé à ses clients abonnés au service « Le Club » (ci-après, les abonnés).

Il ressort de la lecture des différentes brochures du requérant que les patients qui suivent le programme DBC en 24 ou 12 séances sont assimilés aux abonnés : il faut donc en déduire que ces patients profitent également de l'accès privilégié et doivent se plier à la prise d'empreintes digitales.

Lors de l'enregistrement de son abonnement, la personne concernée doit fournir à l'hôtesse d'accueil un ensemble de données déterminées : elle se fait photographier et remet ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires et une donnée biométrique, à savoir une image de son empreinte digitale.

La Commission note qu'il ressort des plaintes qu'elle a reçues que les personnes ayant souscrit un abonnement avant le 21 septembre 2005 doivent également remettre leurs données biométriques lors de leur première visite après le 21 septembre 2005.

Pour enregistrer ladite donnée biométrique, le futur abonné doit déposer son doigt sur le capteur d'un appareil du requérant. De préférence, l'abonné doit remettre son index droit, mais l'abonné peut choisir de poser un autre doigt (par exemple à cause d'une mutilation).

Cet appareil capture l'image de l'empreinte. Suivant la demande d'autorisation,, le logiciel contenu dans l'appareil enregistreur extrait uniquement quatre minuties (ce que le requérant appelle dans sa demande les "4 Points de Comparaison"). Une minutie est l'arrangement particulier des lignes papillaires formant des points caractéristiques à l'origine de l'individualité des dessins digitaux (ex. arrêt de lignes, bifurcations, lacs, îlots, points). Le logiciel va ensuite calculer, à partir de ces quatre minuties, une valeur de contrôle grâce à une formule algorithmique ; cette valeur est une suite numérique qui est appelée gabarit ou valeur de référence. L'image de l'empreinte est dès lors transformée en gabarit. Il résulte de la demande que le logiciel va sauvegarder le gabarit et que l'image de l'empreinte digitale est détruite.

Le processus relatif à l'empreinte digitale ci-avant décrit constitue l'enrôlement.

Toutes les données collectées – et notamment le gabarit – sont centralisées dans une base de données unique. Cette base de données enregistrera également les services reçus par l'abonné dans les installations du Centre thermal. Chaque abonné est reconnu par un numéro d'identification unique.

A l'issue de son enregistrement, l'abonné se voit remettre un bracelet-chip sur lequel figure uniquement son numéro d'identification.

L'abonné se présente avec son bracelet-chip devant les bornes qui lui sont réservées près des tourniquets : il présente son bracelet devant la borne.

Cette opération permet de reconnaître la personne dans la base de données : les données de cette personne sont alors « extraites ».

Ensuite, le capteur se trouvant sur la borne va capter l'image de l'empreinte du même doigt que l'abonné a choisi lors de l'enrôlement.

Le logiciel contenu dans la borne va alors scanner l'image digitale et, après avoir appliqué la formule algorithmique choisie pour l'enrôlement, la comparer aux données de l'abonné enregistrées dans la base de données.

Le tourniquet est débloqué si la comparaison des deux empreintes est positive.

Compte tenu de la particularité du traitement envisagé, la Commission nationale a recouru aux services d'un consultant indépendant pour la conseiller dans les questions techniques et de sécurité : une visite des lieux s'est déroulée le 28 novembre 2005 en présence notamment de représentants de la direction du Centre thermal.

Le consultant a examiné les modalités et caractéristiques techniques du système et remis un rapport détaillé à la Commission nationale dans lequel il a relevé notamment qu'il ne peut pas exclure sans laisser des doutes qu'outre les minuties, l'empreinte digitale intégrale soit stockée dans la base de données. La documentation technique et exhaustive communiquée par le requérant précise qu'à

chaque passage sur le capteur l'image de l'empreinte digitale est enregistrée. Si l'image scannée à la borne est plus nette et précise que le gabarit celui-ci est effacé et l'image nouvellement scannée va alors servir de référence pour les comparaisons ultérieures.

A l'expiration de la validité de son abonnement, toutes les données à caractère personnel de l'abonné sont supprimées de la base de données.

1. A titre préliminaire : l'applicabilité de la loi

Les traitements contenant des données biométriques ne sont pas expressément prévus par la loi du 2 août 2002. Par conséquent, il y a lieu de vérifier, à titre préliminaire, si ladite loi a vocation à s'appliquer.

a) Donnée biométrique et donnée à caractère personnel

Il se pose la question de savoir si une donnée biométrique répond à la définition de données à caractère personnel donnée par la loi du 2 août 2002.

La biométrie est « *l'exploitation automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité* » (IBG, International Biometric Group).

La biométrie est donc la transformation des caractéristiques physiques d'un individu en une suite numérique.

Il a été précisé que les systèmes biométriques sont « *des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche)* » (CNIL, 22e rapport d'activité 2001, « un siècle de biométrie »).

Une donnée biométrique est donc une caractéristique physique d'un individu qui est traduite en une suite informatique et numérique.

L'article 2, lettre (e), de la loi définit la donnée à caractère personnel comme « *toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (" personne concernée") ; une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique* ».

La Commission Nationale de l'Informatique et des Libertés (ci-après : CNIL) a estimé que « *par nature, un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application des lois « informatique et libertés » comme d'autres données personnelles (un nom, une adresse, un numéro de téléphone, etc.). La finalité de ces techniques consiste en effet, pour l'essentiel, à reconnaître une*

personne physique, à l'identifier, à l'authentifier, à la repérer » (CNIL, 22e rapport d'activité 2001, p.166).

Le Tribunal de Grande Instance de Paris suit cette définition : dans un jugement du 19 avril 2005 (CE Effe Services, Syndicat Sud Rail c/ Effia Services), il a ainsi décidé qu'une « *empreinte digitale, même partielle, constitue une donnée biométrique morphologique permettant d'identifier les traits spécifiques qui sont uniques et permanents pour chaque individu* ».

En l'espèce, le gabarit de l'empreinte digitale figure dans la base de données centralisée.

Par conséquent, et au vu des développements ci-avant exposés, l'image d'une empreinte digitale et le gabarit sont des données à caractère personnel telles que définies par la loi du 2 août 2002.

b) Le traitement de données au sens de la loi et le traitement de données biométriques

Il convient de déterminer si un traitement contenant une ou plusieurs donnée(s) biométrique(s) est un traitement au sens de la loi.

L'article 2, lettre (s) de la loi donne une définition précise de la notion de traitement de données à caractère personnel.

En France, la CNIL a retenu que « *lorsque le traitement des données biométriques suppose la conservation et le stockage des gabarits, il y a constitution d'une base de données qui relève alors de l'ensemble des dispositions des lois de protection des données au premier rang desquelles figurent le principe cardinal de la finalité et le principe implicite de nos législations qui en est le corollaire : le principe de proportionnalité* » (CNIL, 22e rapport, p.167). Il échet de préciser que la définition de traitement qui figure dans la loi du 2 août 2002 est identique à celle donnée à l'article 2, paragraphe (3) de la loi française coordonnée n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La solution donnée par la CNIL est transposable à notre législation.

Dès lors, le traitement de données biométriques envisagé par le requérant est à qualifier de traitement de données à caractère personnel et la loi du 2 août 2002 a vocation à s'appliquer.

c) La qualification du traitement envisagé par le requérant

L'article 2, lettre (q), de la loi définit la surveillance comme « *toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer des mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile* ».

Il ressort des travaux parlementaires que « *le projet de loi [n°4735] inclut les traitements de données à des fins de surveillance comme par exemple la vidéosurveillance ainsi que toute forme de surveillance électronique* » (n°4735/0 p.36 et 4735/13 p.97).

La doctrine a retenu que la surveillance des mouvements vise « *tous les dispositifs permettant de détecter les mouvements des personnes. Outre les caméras, tombent dans cette catégorie des détecteurs de mouvements, à condition toutefois qu'ils permettent d'identifier, directement ou non, une personne. Sont surtout visés ici les (…) portiques et points de passage qui identifient les personnes qui les franchissent* » (La Protection des données personnelles, Cyril Pierre-Beausse, éd. Promoculture, n°162).

En l'espèce, le système décrit dans la demande d'autorisation, utilise une borne d'accès qui détecte et enregistre les mouvements des personnes (abonnés, curistes DBC) saisies dans le fichier afférent voulant accéder aux installations du « Club ».

Par conséquent, il s'agit d'un traitement à des fins de surveillance : le traitement envisagé tombe dans le champ d'application de l'article 10 de la loi.

2. Finalité et légitimité du traitement envisagé

a) Finalité

Les finalités du traitement envisagé sont décrites dans la demande d'autorisation de la manière suivante :

> « *(i) le contrôle de l'accès au Site et la lutte contre la fraude et*
> *(ii) une gestion commerciale optimisée du Site, pour le décompte des entrées sur le compte des Abonnés* »

Aux termes de l'article 4 paragraphe (1) lettre (a) de la loi, le responsable du traitement doit s'assurer que les données sont « *collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ».

Il est vrai que la fraude peut avoir des conséquences préjudiciables, voire ébranler la pérennité économique d'une exploitation. En effet, d'une part, l'exploitant est contraint de répercuter le coût que représente pour lui la fraude sur les personnes qui profitent licitement de son installation : le prix des prestations est ainsi majoré pour compenser les pertes financières causées directement par la fraude. D'autre part, la tolérance de la fraude donne une mauvaise image du professionnel : plus la fraude est facile, plus elle incite également les contrevenants à revenir et cela ouvre des perspectives à des personnes mal intentionnées qui voudraient profiter illicitement des installations. Dès lors, la volonté d'éliminer les risques de fraude rassure également les personnes qui ne fraudent pas et qui payent leurs prestations sans poser de difficultés.

Le requérant a donc un intérêt économique évident à profiter de l'évolution technologique pour combattre la fraude et optimiser le fonctionnement de son entreprise.

Les impératifs légitimes qu'il avance sur le plan de la gestion commerciale comprend tant la recherche du confort des abonnés qui se rendent dans les installations que la réduction des coûts économiques liés à la diminution du

personnel qui contrôlaient physiquement les flux des personnes entrant dans le site, et plus particulièrement, le flux des abonnés.

Au vu de ce qui précède, la Commission nationale considère que **les finalités décrites dans la demande d'autorisation sont déterminées, explicites et légitimes au sens de l'article 4 paragraphe (1) lettre (a) de la loi**.

Elle rappelle toutefois que, conformément à l'article 4 de la loi précitée, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées.

b) Légitimité

La Commission nationale note qu'un traitement à des fins de surveillance (que ce soit le régime général visé à l'article 10 ou le régime particulier prévu à l'article 11) doit, pour être licite, être effectué conformément aux dispositions de l'article 4 de la loi (cf. document parlementaire 4735/13, p. 17).

Dérogeant à l'article 5 qui traite des conditions de légitimité générales, l'article 10 de la loi détermine les hypothèses dans lesquelles une surveillance peut être effectuée, lesquelles sont au nombre de trois (cf. document parlementaire 4735/13, p. 17). Les cas d'ouverture permettant cette surveillance sont limitatifs (cf. document parlementaire 4735/00, p. 98).

En l'espèce, la demande d'autorisation est basée sur l'article 10, paragraphe (1), lettre (a) de la loi parce « *que les personnes concernées donnent leur consentement à la collecte et au traitement des Données, et en particulier des Points de Comparaison* ».

La notion de consentement figurant à l'article 2, lettre (c), de la loi est plus rigoureuse que celle donnée par la directive 95/46/CE : la loi définit en effet le consentement comme « *toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée (…) accepte que les données à caractère personnel fassent l'objet d'un traitement.* »

Dans sa demande, le requérant précise que le consentement, « *recueilli lors de la souscription à un abonnement* » est « *(a) informé, au moyen de la brochure [explicative] ; (b) spécifique, car les conditions générales ne sont applicables qu'à l'accès au Site et les Points de Comparaison sont exclusivement utilisés en vue de la Vérification ; et (c) libre, car celle-ci peuvent choisir un mode d'accès au Site autre que l'abonnement, et ainsi ne pas être soumis à la Vérification.* »

Il convient d'analyser si les éléments constitutifs du consentement tels que définis à l'article 2, lettre (c) de la loi sont effectivement réunies en l'espèce :

- Un consentement exprès et non équivoque

« *Le consentement de la personne au traitement de ses données doit être exprès et non équivoque. Aucune forme écrite et aucune formule sacramentelle ne sont requises.* » (cf. Doc. Parl. 4735/13).

Il en résulte qu'un **consentement implicite ou tacite ne répond pas aux exigences de la loi et n'est dès lors pas suffisant pour légitimer un traitement de données**.

Il résulte de la demande que le préposé du requérant recueille directement le consentement exprès et non équivoque des abonnés.

La Commission nationale estime donc que le consentement des abonnés est exprès et non équivoque.

- Un consentement <u>libre</u>

Le Code civil ne définit pas la notion de consentement.

La doctrine retient que le terme consentement désigne « *la manifestation de volonté de chacune des parties, l'acquiescement qu'elle donne aux conditions du contrat projeté. C'est avec cette signification que le mot consentement est employé lorsqu'on parle de « l'échange de consentements » ou encore lorsqu'on dit d'une personne qu'elle « a donné consentement* » (Les obligations, Précis Dalloz, extrait n°85).

Il ressort des travaux parlementaires que les articles 1112 et suivants du Code civil doivent servir de lignes directrices pour apprécier le caractère libre du consentement (cf. doc. parl. 4735/13, p.5).

L'article 1112, alinéa 1er, du Code civil dispose qu'il « y a violence lorsqu'elle est de nature à faire impression sur une personne raisonnable, et qu'elle peut lui inspirer la crainte d'exposer sa personne ou sa fortune à un mal considérable et présent ».

La jurisprudence luxembourgeoise retient qu'il « *n'y a violence que lorsque celle-ci atteint un degré de gravité suffisant et qu'il existe un danger raisonnable pour la personne ou les biens du contractant* » (Tribunal d'arrondissement de Luxembourg, 7 avril 1948, 14, 399).

Il faut en conclure que la notion de violence – et donc l'absence de consentement libre – est entendue de façon très restrictive.

Or, la théorie générale dégagée en droit civil n'est pas transposable à la matière spécifique de la protection des données pour apprécier si un consentement est libre.

En effet, les travaux parlementaires précisent encore que « *la liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce* » et, comme il a déjà été dit, que les articles 1112 et suivants du Code civil doivent **<u>servir de lignes directrices</u>** en la matière.

La doctrine retient en effet qu'en matière de protection des données, la contrainte « *peut découler de la situation juridique ou économique dans laquelle est placée la personne concernée, par rapport au responsable du traitement* » (La Protection des Données Personnelles, Cyril Pierre-Beausse, Promoculture 2005, extrait 74).

Ainsi, «*dans une situation économique qui met en relation une personne faible (la personne concernée) et une personne dominante (le responsable du traitement), comme, par exemple, lors de l'obligation de contracter un prêt bancaire ou une*

assurance-vie, peut-il s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre, alors qu'il lui est demandé de fournir telle ou telle donnée à caractère personnel « nécessaire » pour que la conclusion du contrat qui entraînera la prestation de service nécessitée puisse avoir lieu. De ce fait, le consentement de la personne concernée est une condition primordiale de licéité d'un traitement de données à caractère personnel. » (doc. parl. 4735/0, p.27).

La contrainte (sous laquelle le consentement peut être recueilli) peut donc résulter de la situation juridique ou économique dans laquelle se trouve la personne concernée par rapport au responsable du traitement.

La doctrine retient que « *l'utilisation de la biométrie doit demeurer volontaire. Le consentement doit être libre, spécifique et informé. Cela suppose que le consommateur (la personne concernée) ait à disposition d'autres alternatives s'il ne souhaite pas que des données biométriques le concernant soient collectées et traitées. (…) Le consentement sera en particulier libre si elle* [la personne concernée] *n'éprouve pas de réticence par rapport à l'utilisation des données biométriques la concernant. Lorsqu'il n'est pas possible d'obtenir un consentement libre, notamment lorsque la personne concernée se trouve dans une situation de subordination ou dans un rapport déséquilibré qui ne lui laisse pas de véritable choix, (…) le recours à la biométrie ne peut intervenir que si la loi le prévoit…* » (Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé, Jean-Philippe Walter, 26e Conférence internationale des Commissaires à la protection des données et à la vie privée, septembre 2004, p.8).

Pour que le consentement soit libre, encore faut-il que le requérant offre des alternatives aux personnes qui refusent le traitement de leurs données biométriques.

En l'espèce, les abonnés qui refusent de remettre leurs données biométriques ont la possibilité d'accéder aux installations mais uniquement en payant plus cher le service (par exemple une entrée journalière ou un carnet à entrées multiples). La possibilité de prendre un abonnement sans devoir se soumettre à la prise d'empreintes digitales n'est pas offerte.

Il convient de remarquer en outre que le requérant a une position unique au Luxembourg. Le requérant est un établissement public, certes à caractère industriel et commercial, qui, financièrement, doit tenir en équilibre son exploitation, mais qui en même temps exerce une mission d'intérêt public. Le requérant occupe sur le marché du Grand-Duché de Luxembourg une place que l'on peut considérer comme unique, entre autres de par sa taille et la diversité de ses services. Il s'agit par ailleurs du seul établissement « thermal » au Grand-Duché » et il n'existe pas d'autres établissements comparables à celui du requérant. Les curistes doivent, obligatoirement venir suivre leur programme chez le requérant. Dès lors, on peut considérer que le requérant est en position quasi monopolistique au Grand-Duché, alors qu'il n'existe pas de concurrent potentiel offrant des prestations tout à fait identiques.

Le consentement des patients suivant le traitement médical DBC pourrait être contraint alors qu'ils ont d'abord choisi de suivre un programme médical – programme que le requérant est le seul à le proposer au Grand-Duché -, et que ce programme sous-entend la condition d'abonné : se trouvant devant un fait accompli

ils n'ont pas d'autre choix que celui d'être soumis à un traitement de données biométriques.

Compte tenu de ces éléments, la Commission nationale s'interroge sur le point de savoir si le consentement des personnes concernées peut dans tous les cas être considéré comme étant donné de façon absolument libre.

- Un consentement spécifique et informé

« Le consentement doit être spécifique, en ce qu'il ne peut porter que sur des traitements déterminés. C'est dans cette optique que le responsable du traitement doit informer la personne concernée sur la ou les finalités déterminées du traitement auquel les données sont destinées. Si plusieurs finalités sont poursuivies par un même traitement, le responsable du traitement doit en informer la personne concernée. » (cf. Doc. Parl. 4735/13).

Le droit à l'information est une notion essentielle de la loi.

« La personne concernée doit [en effet] donner son consentement en connaissance de cause, ce qui explique une nouvelle fois le lien entre le consentement de la personne concernée avec le principe de la qualité des données prévu à l'article 4, paragraphe (1) lettre (a), et avec le droit à l'information prévu à l'article 26. Ce droit à l'information doit s'exercer soit lors de la collecte des données auprès de la personne concernée, soit lors de l'enregistrement ou la première communication à un tiers pour les données qui n'ont pas été collectées auprès de la personne concernée. » (cf. Doc. Parl. 4735/13).

En vertu de l'article 10, paragraphe (2) et l'article 26 de la loi, le responsable du traitement doit informer les personnes concernées de la mise en œuvre de la surveillance.

Le droit à l'information implique que la personne concernée soit informée de ce qui suit :

« (a) l'identité du responsable du traitement, et le cas échéant, de son représentant ;
(b) la ou les finalités déterminées du traitement auquel les données sont destinées ;
(c) toute autre information supplémentaire telle que :
- *les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;*
- *le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ;*
- *l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;*
- *la durée de conservation des données ».*

De plus, il convient d'apprécier *in concreto* la liste des informations supplémentaires telles que prévues à la lettre (c). Ainsi, « *le responsable du traitement devra fournir* ***toutes les informations supplémentaires nécessaires*** *compte tenu des circonstances particulières dans lesquelles les données sont collectées, pour assurer à l'égard de la personne concernée un traitement loyal des données, c'est-à-dire une information pleine et entière. La liste de ces informations supplémentaires n'est pas exhaustive.* » (travaux parlementaires, 4735/13, page 24).

La Commission estime que, compte tenu de la nature sensible des données biométriques, l'information doit également porter sur l'existence et la catégorie de destinataires à qui les données sont communiquées ainsi que sur la durée de conservation et sur l'existence du droit d'accès et sur le fait que les données sont centralisées. Le requérant doit également informer les personnes concernées sur le fait qu'à chaque passage à la borne, leur empreinte digitale est enregistrée et que si elle est plus précise que celle qui figure dans la base de données, alors la nouvelle image sera sauvegardée et sera utilisée pour les comparaisons ultérieures.

En outre, « *le principe d'un traitement loyal des données à caractère personnel suppose que la personne concernée soit informée des aspects du traitement qui sont pertinents pour elle. Les propriétés du système qui reposent de façon inhérente sur des probabilités et donc sont faillibles, constituent un tel aspect pertinent. Aussi, il revient au responsable du traitement d'informer la personne concernée sur ce fait et sur ce qu'elle peut faire si elle est victime de ce système. Toute présomption d'infaillibilité est erronée* » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005, Conseil de l'Europe, extrait n°31).

En effet, le résultat d'une comparaison est toujours une estimation. La personne concernée doit dès lors être informée lors de la collecte qu'il existe un pourcentage d'échec de reconnaissance de son gabarit. Dès lors, la Commission nationale considère que le requérant doit avertir les personnes concernées de la possibilité que leur donnée biométrique ne soit pas reconnue lors de l'opération de comparaison des gabarits.

Le droit à l'information est une obligation de **résultat**, de sorte qu'en cas de contestation, le requérant devra rapporter la preuve que la personne concernée a été informée (travaux parlementaires, 4735/13, page 24).

« Bien souvent, la crainte qu'une parfaite information ne conduise les personnes à refuser de consentir ou une certaine approche commerciale du problème peuvent contribuer à dégrader l'exigence du consentement » (Acadaméie des Sciences Morales et Politiques, « Société d'information et vie privée », Tome 3, Chapitre 1, « La protection des données personnelles à la croisée des chemins », édition Presses Universitaires de France, Michel GENTOT).

La demande d'autorisation précise que :

> « *Le consentement est recueilli lors de la souscription à un abonnement. A ce titre, chaque personne concernée se voit remettre une brochure explicative sur les conditions de fonctionnement du Système. (…)* ».

De plus, le requérant expose ce qui suit dans sa lettre d'accompagnement à la demande d'autorisation du 31 octobre 2005 :

> « *[le requérant] est déterminé à mettre en place et à diffuser systématiquement des supports d'information clairs et complets sur le Système, ainsi qu'à répondre promptement à toute demande d'information émanant du public* ».

La brochure explicative à laquelle le requérant se réfère précise en effet que les données personnelles et les empreintes digitales seront recensées lors de la

première visite. Mais, elle ne donne pas d'information sur les finalités du traitement, sur une communication ou non à des destinataires, sur l'enregistrement des données d'identification, y compris biométriques dans une base de données centrale, sur l'existence d'un taux d'erreur, sur la durée de conservation des données et sur l'exercice du droit d'accès. Le droit à l'information étant une obligation de résultat, il appartient au requérant de démontrer qu'il le respecte.

Le contenu de ladite brochure est insuffisant pour satisfaire aux exigences d'un consentement informé. Par ailleurs, les plaintes et réclamations reçues de la part de certains abonnés laissent entendre qu'aucune information ne leur a été donnée avant la saisie de la donnée biométrique, les abonnés étant simplement invités à déposer leur doigt sur un capteur.

En conclusion, la Commission nationale estime que le requérant ne respecte pas toutes les conditions d'un consentement libre, spécifique et informé des personnes auprès desquelles il recueille des données biométriques qu'il enregistre et traite dans le cadre du système de contrôle des accès, plus amplement décrit ci-avant.

3. Qualités des données

a) Loyauté de la collecte et exactitude des données

Dans sa demande le requérant précise ce qui suit :

> *« les Données sont recueillies lors de l'abonnement par un préposé du Domaine Thermal et introduites directement dans la Base de Données. Les Points de Comparaison sont collectés au même moment, au moyen d'un dispositif technique spécifique relié au Système »*

De plus, selon les informations fournies par le requérant, l'empreinte digitale est collectée successivement à trois reprises afin de limiter le risque d'erreur lors de l'enrôlement des données. Il convient de rappeler que les algorithmes sont conçus pour donner une réponse à la comparaison sous la forme d'un pourcentage de coïncidences. Cette multiplication de l'enregistrement améliore ainsi l'exactitude de la donnée biométrique, même si cela ne permet jamais d'écarter totalement les erreurs de reconnaissance de la donnée biométrique.

En outre, lors de chaque passage, la machine sauvegarde l'image de l'empreinte digitale si elle est plus nette et plus précise que celle qui figure sur sa base de données : cela contribue à l'exactitude des données.

Bien qu'il semble que les personnes concernées ne soient pas spécifiquement rendues attentives à cette procédure, la Commission nationale estime que l'ensemble des données du traitement envisagé est collecté de manière loyale, tel que l'exige l'article 4 de la loi.

b) Le principe de proportionnalité

Selon le principe de proportionnalité, tout traitement des données ainsi que toute mesure prise en relation avec ce traitement, doit être proportionné aux finalités poursuivies. Ce principe implique que le responsable du traitement doit limiter le

traitement à des données adéquates, pertinentes et non excessives au regard des finalités à atteindre (cf. article 4 paragraphe (1) lettre (b) de la loi).

- **Catégories de personnes concernées**

Il ressort de la lecture des différentes brochures que les patients qui suivent le programme DBC en 24 ou 12 séances sont assimilés aux abonnés.

Par conséquent, et bien que la demande d'autorisation ne le mentionne pas expressément, la Commission nationale estime que les personnes concernées par le traitement envisagé sont les personnes ayant souscrit un abonnement au Club et les patients inscrits au programme DBC en 12 ou 24 séances.

- **Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées**

Le requérant signale que les « *données ne sont communiquées à aucun tiers en vue d'un autre traitement (…) Il n'y a pas de destinataires externes* ».

Il ressort de ce qui précède qu'il n'y a aucun destinataire externe.

Les seuls destinataires relèvent du personnel du requérant, respectivement des personnes placées sous son autorité et qui agissent pour le compte du requérant, lequel précise dans sa demande ce qui suit :

> *« Les personnes susceptibles d'accéder aux Points de Comparaison stockés dans la Base de Données sont :*
> *(a) le responsable du service informatique du Domaine Thermal ; et*
> *(b) le gestionnaire des réseaux du Domaine Thermal*
>
> *(les Destinataires Internes).*
>
> *De manière incidente, un prestataire de services tiers (le fournisseur du Système) peut également accéder (au moins en théorie) au Système lors d'opérations de maintenance, mais n'est pas à considérer comme destinataire au sens de la Loi.* »

Dans le protocole du 20 septembre 2005, il est précisé que « *le droit d'accès au logiciel et à la base de données y relative est limitée aux personnes autorisées. Le droit d'accès et le type d'accès dépendent du niveau d'utilisateur défini pour chacun des utilisateurs.*

⇨ *Gestion administrateur du logiciel*

- *Responsable Mondorf Le Club*
- *Secrétaire Responsable Mondorf Le Club (gestion club)*
- *Responsable service informatique*
- *Gestionnaire des réseaux*
- *Remplaçant du gestionnaire des réseaux*
- *Société EWV fournisseur du logiciel*

⇨ *Gestion comptable : Consultation et édition des états financiers*

- *Caissier principal*
- *Caissier remplaçant*

⇨ *Gestion clientèle (réception du club et points de vente)*

- *Hôtesse d'accueil* »

Il ressort par ailleurs de la demande qu'en *« aucun cas les données recueillies ne font l'objet d'un transfert en dehors de l'Union européenne.*»

Les destinataires mentionnés apparaissent aux yeux de la Commission nationale comme étant légitimes, nécessaires et proportionnés au regard des finalités poursuivies.

- **Durée de conservation des données**

Conformément à l'article 4, paragraphe (1) lettre (d) de la loi, les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalités.

Dans sa demande, le requérant précise ce qui suit :

> *« Les Points de comparaison sont conservés pendant la durée de l'abonnement et sont ensuite systématiquement détruits* ».

Compte tenu du fait qu'à chaque passage à la borne, le logiciel enregistre l'image de l'empreinte digitale et la conserve si elle est plus nette et précise que celle qui figurait préalablement dans la base de données, la Commission nationale tire la conclusion que la donnée biométrique est effacée si, lors d'une comparaison, l'image nouvelle est plus nette. En toute hypothèse et au plus tard, la donnée biométrique est effacée à la fin de l'abonnement.

Par conséquent, la Commission nationale estime que la durée de conservation n'est pas excessive.

- **Proportionnalité d'un traitement contenant des données biométriques**

Dans le cas spécifique des traitements de données biométriques, il est retenu que « *la biométrie, à l'instar de toutes les technologies, est définie par son usage. Les technologies biométriques ne sont, en elles-mêmes, ni nécessairement préjudiciables ni nécessairement favorables à la protection de la vie privée. L'application de ces technologies soulève néanmoins plusieurs problèmes de protection de la vie privée particuliers* » (Groupe de travail sur la sécurité de l'information et la vie privée, Technologies fondées sur la biométrie, OCDE, 10 juin 2005, p.13).

En effet, « *une mesure biométrique est plus qu'un identifiant numérique [car elle] livre des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général* » (Commission d'accès à l'information du Québec, La biométrie au Québec : les enjeux » Document d'analyse, juillet 2002).

Par conséquent, les personnes concernées doivent physiquement se soumettre à chaque passage pour s'identifier. De plus, les données biométriques sont collectées à partir du corps humain.

Il convient de souligner que « *l'intégralité du corps humain et la manière dont il est utilisé par la biométrie constituent un aspect de la* ***dignité humaine*** » (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, Conseil de l'Europe, février 2005, point n°9).

Le Professeur Roger Clarke de l'Australian National University, estime aussi que le recours à la biométrie présente des dangers particuliers pouvant être regroupés en deux catégories. La première est inhérente aux menaces liées à tous les systèmes informatiques (collecte des données sur les individus, multiplication des informations sur leur comportement, leurs déplacements, les actions…), la seconde "s'attache aux caractéristiques propres à la biométrie : celle-ci donne une information intrinsèquement liée à la personne elle-même (distinction entre "information about the person" et "information of the person") ; la personne doit se soumettre physiquement au processus de vérification. Dès lors, la personne concernée doit coopérer : elle doit physiquement se soumettre à la surveillance.

Du fait de l'intrusion particulière dans la sphère privée, qu'elle implique parfois même une atteinte à la dignité humaine et afin de ne pas banaliser son recours, « *la biométrie ne doit* ***pas être utilisée seulement parce qu'elle est pratique, mais parce qu'elle constitue le seul moyen d'atteindre le résultat recherché*** » (Rapport d'information n°439 du Sénat, session 2004-2005, sur la nouvelle génération de documents d'identité et de la fraude documentaire, p.92).

En d'autres mots, « *des données biométriques ne doivent être utilisées que si leur* ***utilisation est adéquate, pertinente et non excessive, ce qui implique une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées*** » (Document de travail sur la biométrie, du 1er août 2003, Groupe de travail « Article 29 » sur la protection des données, n°12168/02/FR GT 80, p.8).

Le degré d'intrusion dans la vie privée diffère en fonction du traitement de données biométriques choisi : il existe en effet une diversité de traitements possibles de données biométriques qui sont plus ou moins intrusifs dans la vie privée des personnes concernées.

La Commission nationale doit dès lors vérifier ci-après si le traitement envisagé par le requérant est proportionné par rapport aux buts recherchés. Il convient de rappeler que la Commission a pour mission de contrôler la proportionnalité des traitements soumis à son autorisation. La jurisprudence luxembourgeoise retient à cet effet que « *la CNPD doit nécessairement procéder à un contrôle de la proportionnalité des mesures envisagées pour décider si le traitement ainsi préconisé est nécessaire pour assurer les besoins prévus par la loi* » (Cour administrative, 12 juillet 2005, rôle 19234 C).

- **Catégories de données**

  - Les catégories de données décrites par le requérant dans sa demande d'autorisation

A ce sujet, le requérant indique ce qui suit :

> *« Les catégories de Données qui n'ont pas de rapport direct avec la surveillance (c'est-à-dire, les données nécessaires au traitement commercial) ne sont pas détaillées ici et font l'objet d'une notification séparée. Les seules Données pertinentes dans le contexte de la présente demande sont les Points de Comparaison. (…)* ».

Malgré l'affirmation du requérant, les données figurant dans la notification susmentionnée sont nécessaires dans le cadre de la présente demande.

L'accès aux installations n'est possible que si l'empreinte digitale est reconnue dans la base de données comme appartenant à l'individu portant le numéro d'identification figurant sur son bracelet.

Il n'y a donc qu'un seul traitement qui comprend la donnée biométrique et les données décrites dans la notification. D'ailleurs le requérant se réfère à la donnée biométrique dans sa notification.

Afin de se prononcer en pleine connaissance de cause, la Commission nationale considère que les données concernant le traitement envisagé sont toutes les données figurant dans la notification (données d'identification, données financières, photographie et donnée biométrique) et le numéro d'identification.

  - La spécificité de l'empreinte digitale comme donnée biométrique

La CNIL a retenu que « *l'empreinte digitale est presque aussi redoutable que les traces ADN car elle est omniprésente : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence* ».

A « *la différence d'autres données biométriques, [les empreintes digitales]* ***laissent des traces*** *qui peuvent être exploitées pour l'identification des personnes et que dès lors toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première* » (CNIL, 21e Rapport d'activité, 2000, p.102).

Le risque de dérive est potentiellement plus élevé quand les données biométriques laissent des traces parce qu'elles peuvent « *être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou eu en main (…)* » (Rapport de la CNIL du 9 décembre 2003 relatif à la demande d'avis 859.794, p.5).

Il convient de rappeler que toutes les données biométriques ne laissent pas de traces (par exemple, le contour de la main, l'iris, la rétine). Ces données ne présentent pas les mêmes dangers que les données qui laissent des traces : « *une base de données de reconnaissance de la voix, de gabarit d'iris, de rétine ou du contour de la main ne peut en aucun cas être utilisée à d'autres fins que de la reconnaissance et d'authentification des personnes qui se présentent devant le*

capteur » (CNIL, 22e rapport d'activité 2001, p.168). Dans ce cas, le risque de dérive et de détournement de finalité est, dès lors, sans intérêt.

Par conséquent, et en raison du risque très limité de l'exploitation ultérieure de données biométriques qui ne laissent pas de traces, les traitements incluant de telles données ne laissant pas de traces sont facilement acceptables.

Ainsi, en Grèce, l'«*Authority for the Protection of Personal Data* » (APPA) a précisé dans sa décision n°9/2003 du 31 mars 2003 qu'elle encourage les traitements qui ne laissent pas de traces (« *Operational recommandations encourage taking advantage of " mild" biometric technologies based on characteristics that do not leave any traces* »).

La Commission nationale est *a priori plus favorable à autoriser, au stade actuel des technologies utilisées,* **les traitements de données biométriques qui ne laissent pas de traces** compte tenu des risques moindres d'atteinte à la sécurité des données et de détournement de finalité. Ces traitements sont en outre ressentis par les personnes concernées comme bien moins intrusifs dans leur vie privée.

La Commission ne partage pas le raisonnement du requérant quand il prétend que « *la collecte des seuls Points de Comparaison place le Domaine Thermal (ou les tiers qui, par impossible, pourraient accéder de manière non autorisée au Système et/ou à la base de Données, ou encore au contenu de la Carte en cas de perte ou de vol de celle-ci) dans l'impossibilité de reproduire l'Empreinte ni de l'utiliser à d'autres fins que la vérification effectuée lorsque l'Abonné sollicite l'accès au Site. Le risque de divulgation de données biométriques relatives aux Abonnés est donc inexistant* ».

Il est vrai que « *la transformation d'une empreinte digitale en gabarit est irréversible, il n'y a aucun risque de reconstitution d'empreinte à partir d'un gabarit* » (8e rapport d'activité du Préposé fédéral à la protection des données en Suisse).

Mais une empreinte digitale est très facile à extraire (par exemple sur un verre) : il existe donc un risque qu'une empreinte soit collectée et d'y appliquer un algorithme précis pour voir si le gabarit est reconnu dans la base de données qui utilise cet algorithme, et ainsi obtenir les données à caractère personnel de cette personne.

De plus, lors de la visite sur les lieux, le requérant n'a pas donné la certitude que l'image non cryptée de l'empreinte n'était pas sauvegardée dans la base de données. Le consultant indépendant affirme ainsi qu'il « *ne peut pas être exclu que des informations suffisantes pour reproduire une empreinte ne sont pas enregistrées dans le système. La quantité de données sauvegardées du « fused image » n'est pas indiquée dans la documentation* ».

Par conséquent, la transformation de l'image de l'empreinte digitale en gabarit n'exclut pas l'utilisation des données à caractère personnel à des fins détournées.

- La proportionnalité en termes d'opérations de traitement : la centralisation des données biométriques

Dans sa demande, le requérant a indiqué que le traitement envisagé avait deux finalités, à savoir, d'une part, le contrôle de l'accès au site et la lutte contre la fraude (c'est-à-dire que le titulaire du bracelet-chip est bien la personne qui se présente aux installations) et, d'autre part, la gestion commerciale du site relative au décompte des entrées des abonnés.

La Commission nationale reconnaît que le requérant doit pouvoir apprécier le traitement qu'il estime le plus approprié pour parer à la fraude, pour optimiser le fonctionnement de l'établissement et gérer commercialement son site, deux finalités qui sont tout à fait légitimes pour un acteur économique de son envergure.

Mais les moyens adoptés par le requérant pour atteindre ces finalités doivent être les plus respectueux possible des droits fondamentaux et des libertés de la personne concernée : or, tout système centralisé de données – comme le traitement envisagé par le requérant - présente un risque particulier de dérive, qui n'existe pas quand les données ne sont pas centralisées.

Qui plus est, les systèmes de centralisation de données biométriques qui laissent des traces, comme les empreintes digitales, présentent plus de risques pour la protection des libertés et des droits fondamentaux de la personne que les traitements qui ne prévoient pas une telle centralisation.

Ce n'est pas parce qu'un traitement contient des données biométriques que les dangers sont écartés.

Ainsi, les données biométriques « *ont la réputation d'être extrêmement fiables car elles paraissent liées à la présence physique et réelle d'une personne et, à ce titre, seraient donc inaliénables. Il existe réellement une forte probabilité que l'usage des données biométriques permette d'être assuré d'avoir affaire à la bonne personne.* ***Néanmoins****, les falsifications sont toujours possibles. Les empreintes digitales relevées sur un verre peuvent par exemple servir à créer avec de la cire une empreinte analogue sur un support de stockage* » (Rapport d'étape, pré. cit. p.12).

La Deutsche Bank a réalisé une étude (Deutsche Bank Research « *Biométrie, mythe et réalité », 22 mai 2002*) qui met en exergue les défauts des systèmes biométriques. Ces derniers sont soumis aux mêmes types d'attaques ou de manipulations. Un « *hacker* » peut ainsi intercepter le gabarit de référence ou le gabarit présenté lors de la phase de comparaison. Néanmoins les conséquences ne sont pas les mêmes car, si un nouveau mot de passe ou un nouveau code peuvent être attribués, la caractéristique biométrique ne peut être modifiée.

Dès lors, le recours à un traitement de données biométriques n'écarte pas le **risque de réutilisation des données** centralisées. Mais les conséquences peuvent être particulièrement dommageables lorsqu'il s'agit de données biométriques qui laissent des traces.

Les données biométriques qui laissent des traces permettent en effet de remonter à une personne déterminée.

Comme pour tout traitement de données, « *la conservation dans un traitement des empreintes digitales est susceptible d'être utilisée à des fins étrangères à la finalité que son concepteur lui avait initialement assignée. En effet, et à la différence d'autres données biométriques (…) les empreintes digitales laissent des traces de chacun de nos gestes les plus quotidiens et peuvent être exploitées à des fins d'identification et de recherche des personnes. Dès lors, une base de données d'empreintes digitales, quelle que soit la finalité initiale de sa constitution, est susceptible d'être utilisée à des fins de police. (…) Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est pas tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale.* ***Il pourrait presque être soutenu que l'empreinte digitale est (…) une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers*** » (Rapport d'ensemble relatif à diverses applications de contrôle d'accès utilisant un dispositif de reconnaissance des empreintes digitales, CNIL, 20 octobre 2000, p.2 et 6).

Il a encore été précisé qu'une « *société qui favoriserait le développement de bases de données d'empreintes digitales par exemple, offrirait des moyens considérables et nouveaux - au moins dans l'ordre des « possibles » - d'investigations policières sans forcément qu'un tel objectif ait été initialement recherché. Non pas que les bases de données ainsi constituées l'auraient été à des fins policières mais parce que de telles bases de données, apparemment tout à fait anodines, pourraient être utilisées par la police comme élément de comparaison et de recherche dans le cadre de ses investigations* » (CNIL, 22e rapport d'activité 2001, p.108).

Il faut éviter autant que possible tout risque de réutilisation des données biométriques qui permettent de retrouver facilement un individu en particulier.

Ainsi, la CNIL accepte les traitements de données biométriques ayant pour but la vérification des personnes uniquement lorsque le gabarit d'une empreinte digitale est stocké sur un support individuel exclusivement détenu par la personne concernée et dont celle-ci décide librement de l'utilisation (par exemple, délibérations n°03-015 du 24 avril 2003 et n°2005-115 du 7 juin 2005).

Le Groupe de travail « Article 29 » sur la protection des données a pris position sur les deux systèmes : il est « *d'avis que l'utilisation, à des fins de contrôle d'accès (…), de systèmes biométriques se référant à des caractéristiques qui ne laissent pas de traces (par exemple la forme de la main, mais non les empreintes digitales) ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas enregistrées dans une mémoire détenue par une personne autre que la personne concernée (autrement dit, les données ne sont pas mises en mémoire dans le dispositif de contrôle d'accès ou dans une base de données centrale), crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne* » (Document de travail sur la biométrie adopté le 1er août 2003, n°12168/02/FR, p.7).

En **Allemagne**, le « *Landesbeauftragte für den Datenschutz Niedersachsen* » a écrit dans son rapport n°17 pour l'année 2003-2004 ce qui suit :

> *« Datenschutzprobleme entfallen weitgehend, wenn auf eine zentrale Speicherung verzichtet wird und die Betroffenen das Speichermedium, zum Beispiel eine Chipkarte, selbst verwalten. »*

De plus, Monsieur Peter SCHAAR, „*Bundesbeauftragte für den Datenschutz*", dans le cadre du colloque „Adlershofer Kolloquium" du 28 juin 2005 recommande notamment que „*dass nach Möglichkeit auf eine zentrale Speicherung der Daten verzichtet wird, z. B., durch Speicherung der Daten auf einer Chipkarte oder einem Ausweis*".

Dans le même sens, le Dr. G. Laßmann écrit ce qui suit :

„Werden die biometrischen (Referenz-)Daten beim Nutzer (z.B. auf einer Chipkarte, einem Token oder einer anderen mobilen Speichereinheit) gespeichert, so hat dieser eher die Möglichkeit der Kontrolle über seine Daten. Ein zentraler Datenbestand birgt dagegen Gefahren für das informationelle Selbstbestimmungsrecht, nicht zuletzt wegen der weitgehenden Übermittlungsbefugnisse im Privatbereich und der umfassenden Datenerhebungsbefugnisse der Strafverfolgungsbehörden. Je mehr Daten zentral abgelegt werden und auf diese zumindest theoretisch zugegriffen werden kann, je größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen entstehen können. ..... Ein weiteres Problem besteht darin, dass zentrale Datenbestände üblicherweise ohne Wissen (und Zutun) des Benutzers ausgewertet werden können, was ebenso dessen Selbstbestimmungsrecht einschränkt. Der Einsatz identischer Verfahren in unterschiedlichen Anwendungen führt für den Nutzer zu erhöhten Risiken, da sein biometrisches Merkmal als ein (im Gegensatz zu Namen und Adresse) unveränderbares Personenkennzeichen verwendet werden und sein jeweiliges Nutzungsverhalten zu einem umfassenden Profil zusammengeführt werden kann. Eine dezentrale Speicherung ist daher in den allermeisten Fällen vorzuziehen." (Dr. G. Laßmann, dans „Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren-Kriterienkatalog", TeleTrusT Deutschland e.V., 10 juillet 2002).

En France, la CNIL ne pose pas non plus le principe du refus de collecte de toute donnée biométrique. Elle ne voit pas d'objection par exemple à ce qu'une base de données contienne les gabarits de données biométriques ne laissant pas de traces tels le contour de la main (par exemple, délibération 2005-064 du 20 avril 2005).

Par contre, elle s'oppose avec véhémence au traitement centralisé de gabarits d'empreintes digitales si un tel traitement n'est pas **justifié par des impératifs sécuritaires des locaux à protéger** (délibération 04-018 du 8 avril 2004 pour un exemple de décision de refus et 04-017 pour un exemple d'avis favorable). La CNIL a ainsi accepté un tel traitement pour la Cogema, la Banque de France, les Aéroports de Paris pour l'entrée dans des zones de haute protection (pour une étude comparative, voir le 22e rapport d'activité 2001, p.170 et la 3e partie du Rapport sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre, annexe 4).

Il est intéressant de citer le cas de la demande d'avis n°859.794 formulée par la mairie de Levallois-Perret et la position arrêtée par la CNIL. Cette mairie avait mis en place un traitement destiné à contrôler l'accès à son « roller-parc » au moyen de la reconnaissance d'une empreinte digitale. Le traitement en question reposait sur

l'identification des personnes qui voulaient se rendre dans le « roller-parc ». La mairie justifiait ce traitement en arguant qu'elle souhaitait avoir un système qui évitait une gestion trop lourde pour contrôler l'accès au site et elle entendait également éviter toute manipulation de cartes qui peuvent être perdues ou volées et écarter aussi tout risque de fraude.

Ces finalités sont les mêmes que celles invoquées par le requérant dans sa demande d'autorisation.

Dans son rapport, du 9 décembre 2003, le rapporteur, Monsieur Maurice Benassayag, a proposé un avis défavorable à ce projet compte tenu de l'absence d'impératif de sécurité à protéger. Suivant cette recommandation, la CNIL a, dans sa délibération n°03-065 du 16 décembre 2003, donné un avis défavorable à ce traitement.

Le risque de détournement est proportionnellement plus important que les intérêts à protéger par le traitement. Accepter un tel traitement pour contrôler l'accès à un roller-parc revenait à accepter tous les traitements centralisant des données biométriques qui laissent des traces. Il y aurait alors une multitude de bases de données susceptibles d'être détournées.

Cette position est justifiée parce que les données biométriques qui laissent des traces peuvent être exploitées pour l'identification des personnes et, dès lors, toute base de données d'empreintes digitales est susceptible d'être utilisée à des fins étrangères à sa finalité première.

Dans un jugement du 19 avril 2005, le Tribunal de Grande Instance de Paris (1 ère chambre sociale, CE Effa Services, Syndicat Sud Rail c/ Effa Services) a posé le principe que l'utilisation d'une empreinte digitale qui « *met en cause le corps humain et [qui] porte ainsi atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés. (…)* ». Il a ainsi jugé que « *le traitement automatisé de ces données (…) à des fins de gestion et de contrôle du temps de présence des salariés n'est ni adapté ni proportionné au but recherché* ».

En **Grèce**, l'autorité grecque pour la protection des données, « *Hellenic Data Protection Authority* », refuse également la centralisation des données biométriques sauf si elle se justifie pour des raisons impérieuses de sécurité (par exemple, décisions n°245/9 du 20 mars 2000 et n°9/2003 du 31 mars 2003).

En **Italie,** l'autorité « *Garante per la protezione dei dati personali* » a également émis un avis défavorable le 21 juillet 2005 à la centralisation des données biométriques sauf s'il n'existe pas d'autres moyens pour parvenir à la finalité recherchée.

En **Suisse**, le Préposé fédéral à la protection des données (PFPD) a eu à se prononcer le 6 juin 2005 sur le projet pilote « *Secure Chek* ». Ce projet a pour but d'améliorer le contrôle de la sécurité des données des passagers et de leurs documents de voyage. Dans le cadre de ce projet, le passager « *porteur d'un passeport est authentifié à l'aide de données biométriques (gabarits), ayant été saisies au guichet d'enregistrement après le contrôle du passeport du passager et enregistrées de façon décentralisée sur une carte à puce (smart card)* » (Résumé du rapport final du 6 juin 2005). Le PFPD apporte une appréciation positive de l'usage

des données biométriques mais précise que « *toute modification du projet Secure Check allant dans le sens d'un stockage centralisé des données biométriques ou d'un stockage de données brutes nécessiterait, sous l'angle de la protection des données,* ***une appréciation différenciée****, qui n'est pas couverte par le présent rapport* ».

Dans son 12ème rapport d'activités 2004/2005, le PFPD recommande de prendre en considération entre autres les principes suivants lors du recours à des données biométriques dans le secteur privé :

« *Il faut privilégier … l'utilisation de données biométriques n'impliquant pas le stockage de gabarits dans une base de données gérée par un responsable de traitement autre que la personne concernée. Cette procédure ne soulève en principe pas de problèmes particuliers du point de vue de la protection des données, dès lors que le gabarit est conservé sur un support dont la personne concernée a l'usage exclusif (carte à puce, téléphone mobile, etc.)*

- Si une base de données est constituée et gérée par un responsable de traitement autre que la personne concernée, l'élément biométrique retenu peut avoir des conséquences sur les libertés et droits fondamentaux. Tel est en particulier le cas lorsque l'élément biométrique laisse des traces, comme l'empreinte digitale. Le recours à un tel élément doit répondre à un intérêt prépondérant qualifié de sécurité.

- En l'absence d'un tel intérêt, il convient de recourir à un élément biométrique qui limite le risque d'abus, tel que celui ne laissant pas de trace, comme le contour de la main ».

- **<u>Conclusion</u>**

Le requérant ne justifie pas dans sa demande que l'efficacité de sa gestion commerciale, l'accès à ses installations ainsi que la prévention de la fraude auraient été moins bien assurés par un système moins attentatoire aux droits et libertés des personnes concernées.

Le requérant aurait d'autres possibilités pour parvenir à remplir ses deux finalités sans avoir à s'immiscer autant dans la vie privée des personnes concernées. Si, pour parvenir aux finalités indiquées dans la demande (à savoir l'accès au site et éliminer les risques de fraude ainsi que la gestion commerciale), le requérant souhaite absolument recourir à un traitement de données biométriques, il pouvait envisager des traitements alternatifs moins intrusifs dans la vie privée des personnes concernées.

La Commission ne verrait en principe pas d'objection à ce que les données biométriques permettant l'identification d'un abonné soient stockées exclusivement sur un support individuel, comme par exemple, le bracelet-chip et ce, sans constitution et utilisation d'une base de données biométriques centralisée. Dans ce cas, la personne concernée a la maîtrise sur ses propres données et décide librement de leur utilisation.

La Commission nationale considère que même la centralisation des données biométriques pourrait être admise comme proportionnée aux finalités indiquées,

dès lors que l'élément biométrique retenu serait de ceux qui ne laissent pas de traces comme, par exemple, le contour de la main.

La constitution de bases de données nominatives associées à des empreintes digitales et son utilisation, même limitée 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 utilisée à des fins étrangères aux finalités initialement poursuivies.

La Commission nationale est d'avis que, compte tenu des risques de dérive importants existant pour les fichiers centralisés de données biométriques laissant des traces, il faut circonscrire le recours à ces traitements : **de tels traitements ne peuvent être autorisés que si le requérant justifie de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger**.

Admettre le traitement envisagé par le requérant, alors qu'il s'agit simplement de surveiller l'accès à une aire de loisirs, à défaut d'impératifs de sécurité prépondérants, pourrait contribuer à la désensibilisation du public, « *en raison d'une utilisation toujours croissante de ces données, aux conséquences que leur traitement peut avoir sur la vie quotidienne* » (Document de travail sur la biométrie, Groupe « Article 29 », p.2). Les personnes se résigneraient à donner leurs empreintes digitales sans vraiment mesurer le danger auquel elles s'exposent en cas de réutilisation ou de détournement des données.

En l'espèce, le requérant ne justifie pas de telles nécessités sécuritaires ou protectrices. D'ailleurs, des traitements moins intrusifs pour la vie privée, et donc plus respectueux de la dignité humaine - comme le recours à un traitement de donnée biométrique qui ne laisse pas de traces ou comme le port de la donnée biométrique sur un support détenu par la personne concernée - auraient pu être envisagés.

Il ne faut pas oublier que les personnes concernées viennent pour leur loisir et/ou leur remise en forme sur le site du requérant ; le requérant envisage qu'à court et à moyen termes, le traitement envisagé intègre les données – notamment biométriques – de 7.000 personnes.

Il n'est pas exclu que des personnes mal intentionnées seront forcément intéressées de posséder une telle base de données comportant 7.000 empreintes digitales pour des raisons très différentes et attentatoires aux droits de ces abonnés.

Par conséquent, et compte tenu de toutes ces considérations, **la Commission nationale estime que le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné aux objectifs poursuivis**.

Pour éviter tout malentendu, la Commission relève que, même dans l'hypothèse où le traitement envisagé serait légitime parce que le consentement serait exprès, non équivoque, libre, spécifique et informé au sens de l'article 10 paragraphe (1) lettre (a), elle ne pourrait pas accorder l'autorisation sollicitée du fait du non respect du principe de proportionnalité tel que défini à l'article 4 de la loi.

4. Mesures de sécurité prévues aux articles 22 et 23 de la loi

L'ensemble des mesures de sécurité doit conférer un *« niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger »* (cf. document parlementaire 4735/13, p.37 et Directive 95/46/CE, article 17, paragraphe 2).

Ces mesures doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités (cf. avis d'initiative de la Commission belge pour la protection de la vie privée relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance, n° de rôle 34/99 du 13/12/1999).

(…)

Nb: La description détaillée permettant d'apprécier le respect des mesures de sécurité prévues aux articles 22 et 23 n'est pas publiée, conformément à l'article 15 de la loi (Publicité des traitements).

III. <u>Mesures immédiates</u>

La loi prévoit que la Commission nationale peut prononcer des sanctions administratives à l'égard des responsables de traitement : l'article 33 paragraphe (1) lettre (c) de la loi prévoit ainsi qu'elle peut « *interdire temporairement ou définitivement un traitement contraire aux dispositions de (...) la loi ou de ses règlements d'exécution* ».

Compte tenu du caractère intrusif du traitement à des fins de surveillance, pour lequel l'autorisation n'est pas accordée, et étant donné que le traitement de données biométriques a d'ores et déjà été mis en œuvre, la poursuite de celui-ci porte atteinte aux libertés et droits fondamentaux des personnes concernées.

Dès lors, la Commission nationale **fait interdiction définitive au requérant de poursuivre le traitement** décrit dans sa demande du 31 octobre 2005 (numéro R002245/A002062).

Compte tenu des développements qui précèdent, la Commission nationale, réunissant ses trois membres effectifs et délibérant à l'unanimité des voix :

- n'autorise pas le traitement de données à caractère personnel sollicité par le requérant dans sa demande du 31 octobre 2005 (numéro R002245/A002062),

- interdit définitivement au requérant de poursuivre le traitement en question en application de l'article 33 paragraphe (1) lettre (c) de la loi.

Ainsi décidé à Luxembourg en date du 21 décembre 2005

La Commission nationale pour la protection des données

Gérard Lommel	Pierre Weimerskirch	Thierry Lallemang
Président	Membre effectif	Membre effectif

<u>Indication des voies de recours</u> (art. 14 PANC)

La présente décision administrative peut faire l'objet d'un <u>recours en annulation dans les **3 mois** qui suivent sa notification</u> à l'administré. Ce recours est à intenter par l'administré devant le tribunal administratif et doit obligatoirement être introduit par le biais du ministère d'avocat à la Cour inscrit auprès de l'un des deux tableaux de l'ordre des avocats.