Délibération n°33/2006 du 12 avril 2006 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 du 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 en date du 1er mars 2006, une demande d'autorisation par l'intermédiaire de son avocat, Maître Cyril Pierre-Beausse, enregistrée sous les références R002445 / A002211, 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.

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

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.

Cette demande intervient suite à la délibération n°89/2005 de la Commission nationale notifiée en date du 21 décembre 2005. Par demande du 31 octobre 2005, enregistrée sous les références R0002245 / A002062, le requérant avait, en effet, demandé à la Commission nationale l'autorisation de pouvoir recourir à un traitement de données à caractère personnel à des fins de surveillance. Ce traitement prévoyait la constitution d'une base de données centralisée contenant des données biométriques, à savoir les gabarits des empreintes digitales des abonnés au service « Le Club ». La Commission nationale n'avait pas autorisé ce traitement parce que le requérant ne justifiait pas de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger susceptibles de justifier le recours à un tel traitement.

II. Objet de la demande et bien-fondé

Description du traitement envisagé

Le requérant entend mettre en place un système d'accès à ses installations réservé à ses clients abonnés au service « Le Club » (ci-après, les abonnés).

Lors de l'enregistrement de son abonnement, le futur abonné doit fournir à l'hôtesse d'accueil un ensemble de données déterminées : il se fait photographier et remet ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires et deux données biométriques, à savoir une image de deux empreintes digitales, de préférence une de chaque main.

Pour enregistrer lesdites données biométriques, le futur abonné doit déposer successivement deux de ses doigts sur un numériseur qui capte l'image de chaque empreinte. Le logiciel du système informatique extrait ensuite des minuties. 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 des 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. Le logiciel renouvelle cette opération avec la seconde empreinte digitale.

Les gabarits en question sont transmis par fréquence radio sécurisée à l'une des deux puces du bracelet-chip dans laquelle ils resteront stockés. Le bracelet-chip reste en la possession exclusive de l'abonné pendant toute la durée de l'abonnement.

Le processus relatif aux empreintes digitales ci-avant décrit constitue l'enrôlement. Suivant la demande, les images des deux empreintes digitales ne sont pas enregistrées pendant cette phase.

Le bracelet-chip contient deux puces électroniques distinctes et autonomes qui ont chacune une fonctionnalité propre.

Sur une de ces deux puces, figurent uniquement les gabarits ci-avant décrits des empreintes digitales de l'abonné détenteur dudit bracelet. Ces données ne sont pas stockées dans une base de données centralisée.

Sur la seconde puce, est enregistré le numéro d'identification de l'abonné qui possède le bracelet-chip. Cette puce permet aussi l'ouverture des casiers des vestiaires. Ce numéro d'identification permet de faire le lien avec les données de la base centralisée du requérant, dans laquelle figurent le numéro d'identification de l'abonné, une photographie, ses données d'identification (nom, prénom, adresse, téléphone), ses données bancaires ainsi que le décompte des services reçus par l'abonné sur le site.

L'abonné, qui souhaite accéder aux installations du requérant, se présente avec son bracelet-chip devant les bornes qui lui sont réservées près des tourniquets : il présente son bracelet-chip devant la borne.

Ensuite, il va placer un des deux doigts choisis lors de l'enrôlement sur le capteur se trouvant sur la borne laquelle contient le même logiciel informatique que celui utilisé lors de l'enrôlement. Le logiciel va appliquer la même formule algorithmique à l'empreinte digitale captée. Le système informatique de la borne va ensuite comparer le gabarit qu'il vient d'obtenir avec chacun des deux gabarits sauvegardés dans le bracelet-chip.

Si la comparaison est positive avec un des deux gabarits en question, alors le tourniquet se débloque et l'abonné a accès aux installations du site du requérant.

Il convient de préciser encore qu'à l'instar du processus d'enrôlement, l'image de l'empreinte digitale captée à la borne n'est pas enregistrée dans le système.

A l'expiration de la validité de son abonnement, la personne concernée choisit, soit de renouveler, soit de mettre fin à son abonnement. Dans la première hypothèse, la personne concernée conserve son bracelet-chip avec les gabarits et le numéro d'identification qui restent sauvegardées. Dans la seconde hypothèse, le requérant récupère le bracelet-chip et efface toutes les données qu'il contient. Dans ce dernier cas, si la personne souhaite, plus tard, souscrire un nouvel abonnement au Club, elle devra renouveler les opérations d'enrôlement ci-avant décrits.

A. Généralités : 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.

Donnée biométrique et donnée à caractère personnel

Il se pose la question de savoir si une donnée biométrique répond à la définition de donnée à caractère personnel telle qu'elle figure dans 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 »).

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* ».

En France, 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 l'une des deux puces du bracelet-chip appartenant au requérant et qui est en la possession de la personne concernée pendant la durée de l'abonnement.

Par conséquent, et au vu des développements ci-avant exposés, le gabarit d'une empreinte digitale est une donnée à caractère personnel telle que définie par la loi du 2 août 2002.

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.

« *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, autorité de contrôle nationale française, est transposable à notre législation.

La Commission nationale considère, dès lors, que 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.

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 abonnés voulant accéder aux installations du « Club ».

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

B. Légitimité du traitement envisagé

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).

La Commission nationale retient qu'en procédant de la sorte, le législateur a entendu effectuer lui-même la mise en balance des intérêts respectifs en précisant dans le texte même des articles 10 et 11 de la loi les circonstances dans lesquelles une surveillance est légitime. Il a donc jugé que dans tous les autres cas l'intérêt ou les droits et libertés fondamentaux de la personne concernée prévalent.

En l'espèce, le requérant indique dans sa demande d'autorisation qu'il renvoie à la condition de légitimité exposée dans sa demande d'autorisation du 31 octobre 2005 (ci-après : « la première demande d'autorisation »).

Le requérant y invoquait l'article 10, paragraphe (1), lettre (a), parce « *que les personnes concernées donnent leur consentement à la collecte et au traitement des Données, et en particulier des Points de Comparaison* ». Il 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.* »

Dans sa demande du 1er mars 2006, le requérant précise aussi que « *l'existence du consentement pourra être déduite de l'acceptation par l'abonné de fournir son empreinte digitale* ». Il indique encore que l'abonné se verra systématiquement remettre une brochure explicative qui contiendra les informations relatives au fonctionnement du traitement envisagé ainsi que les mentions exigées par l'article 26, paragraphe (1), de la loi.

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.* »

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 spécifique et informé

Tout d'abord, *« 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).

Ensuite, le consentement doit être informé. Le droit à l'information est une notion essentielle de la loi. Il s'agit, en plus, d'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) et qu'il a respecté scrupuleusement cette obligation.

« La personne concernée doit 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 d'autres mots, la personne concernée doit avoir été préalablement rendue attentive et renseignée sur tous les aspects du traitement afin de pouvoir donner son consentement en pleine connaissance de cause.

En vertu de l'article 10, paragraphe (2), et l'article 26, paragraphe (1), 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, tel qu'arrêté à l'article 26 de la loi, 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 ; (…)*
- *l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;*
- *la durée de conservation des données ».*

Il convient d'apprécier *in concreto* la liste des **informations supplémentaires** telles que prévues à la lettre (c) : « *le responsable du traitement devra [en effet] 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 des données et sur l'existence du droit d'accès. Le requérant doit également informer les personnes concernées sur le fait que la donnée biométrique n'est à aucun moment enregistrée dans une base de données.

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 également informer les personnes concernées de la possibilité que leur donnée biométrique ne soit pas reconnue lors de l'opération de comparaison des gabarits.

Le requérant a indiqué que les nouveaux abonnés se voient systématiquement remettre une brochure explicative.

La Commission nationale estime que la notice d'information doit être remise avant la souscription à l'abonnement, respectivement concomitamment à la souscription. La brochure doit satisfaire aux remarques ci-avant exposées.

Sous réserve des observations ci-avant formulées, le consentement, collecté tel que décrit dans la demande, peut être considéré comme spécifique et informé au sens de la loi.

- 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 pas suffisant pour légitimer un traitement de données, dès lors qu'il est dépourvu d'une manifestation de volonté active et spécifique.

Le préposé du requérant devra donc recueillir directement le consentement exprès et non équivoque de chacun des abonnés.

- Un consentement libre

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). Ils précisent encore que « *la liberté du consentement doit s'apprécier au cas par cas au regard des circonstances de l'espèce* ».

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).

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.

En l'espèce, les abonnés qui refusent de remettre leurs données biométriques ont la possibilité d'accéder aux installations du « Club » en payant plus cher ses services (par exemple en achetant une entrée journalière ou un carnet à entrées multiples). Le requérant offre donc une alternative aux personnes qui ne souhaitent pas souscrire un abonnement et fournir leurs données à caractère personnel.

Dès lors, la Commission nationale considère que le consentement de chaque abonné est libre au sens de la loi.

En **conclusion**, elle estime que la demande du requérant peut être légitimée sur base de l'article 10, paragraphe (1), lettre (a), de la loi sous réserve des observations qui précèdent.

C. Qualité des données

1. La finalité du traitement

Dans sa demande d'autorisation, le requérant renvoie aux finalités du traitement décrites dans sa première demande d'autorisation. Ces finalités étaient alors décrites 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, et peut 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 invoquées par le requérant 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.

2. Proportionnalité

Selon le principe de proportionnalité, tout traitement des données 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).

a. Catégories de données et traitement envisagé

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, « *le risque le plus actuel de la généralisation du recours à la biométrie est sa banalisation et la tentation de la substituer à d'autres outils de sécurisation tout aussi performants pour des usages précis* » (Pierre Leclercq, A propos de la biométrie, Revue Communication, LexisNexis de mars 2003, p.14 à 18).

Il existe, en effet, un danger supplémentaire lié au traitement contenant des données biométriques : les applications, les risques et les techniques de ces traitements sont mal apprivoisés alors qu'ils resteront longtemps en développement. En l'état actuel des avancées technologiques, toutes les implications des traitements contenant des données biométriques ne sont pas connues.

Dès lors, « *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).

- <u>Les catégories de données décrites par le requérant dans sa demande d'autorisation</u>

A ce sujet, la demande du requérant renvoie à sa première demande d'autorisation qui indiquait 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. (…)* ».

La Commission nationale ne partage pas cet avis, alors qu'elle considère que les données d'identification font également partie du traitement contenant les données biométriques.

- 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 ne laissant pas de traces, les traitements incluant de telles données 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* »).

Il convient de préciser également que le danger lié à l'utilisation des données à caractère personnel à des fins détournées existe encore lorsque l'image de l'empreinte digitale est transformée en gabarit.

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.

- La proportionnalité en termes d'opérations de traitement : les données biométriques enregistrées sur un support individualisé

Le requérant avait initialement envisagé un traitement qui reposait sur la centralisation des données biométriques, et plus particulièrement des gabarits des empreintes digitales. Dans la délibération précitée n°89/2005, la Commission nationale avait retenu qu'à défaut de justifier de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger, le premier traitement envisagé n'était ni adapté ni proportionné aux objectifs poursuivis, à savoir le contrôle de l'accès au site, la lutte contre la fraude ainsi que la gestion commerciale du site relative au décompte des entrées des abonnés.

Le traitement envisagé dans ladite demande du 1er mars 2006 est foncièrement différent. En effet, les gabarits des empreintes digitales ne sont plus centralisés dans une base de données unique contrôlée par le requérant. Désormais, les données biométriques sont stockées dans l'une des deux puces contenues dans le bracelet-chip qui reste en la possession exclusive de l'abonné, c'est-à-dire de la personne concernée par le traitement envisagé par le requérant.

La différence fondamentale entre le premier traitement envisagé et le traitement qui fait l'objet de la demande d'autorisation du 1er mars 2006 est le risque potentiel de réutilisation détournée des données biométriques.

En effet, « *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).

C'est la raison essentielle pour laquelle les traitements de données biométriques non centralisées dans une base de données unique sont, en principe, autorisés par les autorités de contrôle européennes et par les institutions internationales.

Ainsi, 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 **France**, la CNIL accepte les traitements de données biométriques ayant pour but la vérification des personnes uniquement 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).

De même, 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 ».

- **Conclusion relative aux catégories de données et opérations de traitement envisagé**

En l'état actuel des avancées technologiques, et compte tenu du faible risque de réutilisation des données biométriques stockées exclusivement sur un support individuel qui reste en la seule possession de la personne concernée, la Commission nationale considère que le traitement envisagé dans la demande du 1er mars 2006 susmentionnée apparaît comme adapté et proportionné aux objectifs poursuivis.

b. Catégories de personnes concernées

Il ressort de la demande d'autorisation que les personnes concernées par le traitement envisagé sont les personnes ayant souscrit un abonnement au service « Le Club ».

c. Destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées

Le requérant renvoie également à sa première demande d'autorisation dans laquelle il indiquait que les « *données ne sont communiquées à aucun tiers en vue d'un autre traitement (…) Il n'y a pas de destinataires externes* ».

d. 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 :

> *« Lorsque l'abonnement prend fin, le bracelet-chip est désactivé (donc ne permet plus l'accès) mais contient toujours les Minuties. Si la personne concernée (A) renouvelle son abonnement, les Minuties sont conservées et le bracelet-chip est simplement réactivé ; (B) met définitivement fin à son abonnement, le bracelet-chip est restitué au Domaine Thermal et les Minuties sont systématiquement détruites par effacement des données contenus sur le bracelet-chip. »*

Le requérant devra veiller à effacer les données biométriques du bracelet-chip à la fin de l'abonnement, respectivement dès que l'abonné l'aura retourné et au plus tard dans les vingt quatre heures. A ce titre, le requérant indique dans sa demande d'autorisation qu'il « *va mettre en place une procédure obligatoire pour tous les membres de son personnel affecté à l'accueil du public et à la gestion des abonnements (et chargés à ce titre de l'Enrôlement).* »

D. Les droits d'accès et de rectification

Il est acquis que « *toute personne peut **accéder** aux données biométriques qui la concerne (article 8, lettre b, Convention 108). Ce droit s'applique aussi bien aux données biométriques qu'aux données associées qui révèlent, intentionnellement ou non, des informations sur la personne concernée. (…) Accorder le droit d'accès aux données biométriques supposera souvent qu'une machine capable de lire les données biométriques soit à disposition. De même cela pourrait nécessiter un expert pour interpréter et vérifier les données. Le Comité estime que le responsable de traitement ne devrait pas pouvoir refuser de telles demandes au seul motif qu'une machine ou*

un expert ne dont pas disponibles. (Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005, extraits 80 à 82).

Compte tenu des développements qui précèdent, la Commission nationale considère que le requérant devra prendre toutes les mesures techniquement possibles pour garantir aux abonnés le droit d'accès à leurs données à caractère personnel.

Ensuite, en vertu du droit de **rectification** la personne concernée a le droit de demander l'effacement de son gabarit et, corollairement, un nouvel enrôlement de son empreinte digitale dès qu'elle considère que le taux de faux rejets est anormalement élevé.

En effet, la reconnaissance par comparaison de gabarit repose sur la probabilité : « *au cours de la phase d'enrôlement, l'algorithme servant à extraire le gabarit de la caractéristique biométrique peut être plus ou moins étendu selon la finalité du système. Un algorithme moins étendu va accroître la probabilité de fausses acceptations ou de faux rejets puisque le gabarit sera moins spécifique..* » (Rapport d'étape, pré.cit., extrait 88). Dès lors, « *il est possible qu'un conflit survienne entre le responsable du traitement et la personne concernée à propos du degré acceptable de probabilité de faux rejets. Si la personne concernée demande un nouvel enrôlement alors que le responsable de traitement n'admet pas que les données sont inexactes, le droit de rectification pourrait être interprété comme donnant droit en principe à un nouvel enrôlement par la personne concernée sans coûts excessifs. Il en va de même si des données enrôlées étaient correctes, mais que la caractéristiques biométrique a été modifiée avec l'âge, un accident ou de la chirurgie. Au fil du temps, les données sont devenues graduellement incorrecte*s » (id. extrait 93).

En tout état de cause, les droits d'accès et de rectification doivent pouvoir être exercés gratuitement par les abonnés lors de la mise en œuvre du traitement envisagé ou à tout moment et sans formalités contraignantes. De plus, ces droits doivent être étendus aux données associées (comme la date et la localisation de l'utilisation du système et les services utilisés) (cf. Conclusions du rapport d'étape pré. cit., point n°7).

E. Pays tiers à destination desquels les transferts de données sont envisagés

Suivant la demande d'autorisation, aucun transfert vers des pays tiers (hors Union Européenne) n'est envisagé.

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

L'ensemble de ces 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 pour la protection de la vie privée belge, n° de rôle 34/99 du 13/12/1999).

C'est au requérant de prouver qu'il met en place un niveau de sécurité approprié.

En l'espèce, les mesures de sécurité prévues aux articles 22 et 23 de la loi ont fait l'objet d'une description détaillée.

La Commission nationale constate que le contenu de la description relative aux mesures de sécurité satisfait aux exigences des prédits articles.

***

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

délivre l'autorisation sollicitée en matière de traitement de catégories particulières de données en vertu de l'article 10, paragraphe (1), lettre (a), de la loi ;

autorise, dès lors, le Domaine Thermal de Mondorf à recourir au traitement des données envisagé selon les modalités précisées dans sa demande du 1er mars 2006 sous réserve de respecter les conditions suivantes :

- les données biométriques ne doivent pas être enregistrées dans une base de données centralisée mais stockées exclusivement sur un support individuel qui reste en la seule possession de la personne concernée ;

- la brochure explicative devra être remise aux personnes concernées avant la souscription de l'abonnement, respectivement concomitamment à cette souscription ;

- outre les informations obligatoires prévues à l'article 26, paragraphe (1), de la loi, la brochure explicative et/ou les informations fournies oralement devront contenir les éléments suivants :

    - l'existence et la catégorie de destinataires à qui les données sont communiquées ;

    - l'existence du droit d'accès et de rectification ;

    - l'indication que la donnée biométrique n'est pas enregistrée dans une banque de données ;

    - l'existence d'un taux d'erreur de reconnaissance inhérent à tout système incluant des gabarits d'empreintes digitales ;

    - la durée de conservation des données à caractère personnel ;

- le Domaine Thermal de Mondorf devra veiller à effacer les données biométriques du bracelet-chip à la fin de l'abonnement, respectivement dès que l'abonné l'aura retourné et au plus tard dans les vingt quatre heures ;

- plus généralement, les données recueillies doivent être traitées loyalement et ne doivent être utilisées que pour les finalités sur lesquelles est fondée la présente autorisation.

Ainsi décidé à Luxembourg en date du 12 avril 2006.

La Commission nationale pour la protection des données

Gérard Lommel	Pierre Weimerskirch	Thierry Lallemang
Président	Membre effectif	Membre effectif

Indication des voies de recours

La présente décision administrative peut faire l'objet d'un recours en annulation dans les **3 mois** qui suivent sa notification 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.