JdT 2010 I p. 396, 412

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE C. KSS SCHAFFHAUSEN; 4 AOÛT 2009, A-3908/2008 ; ATAF 2009/44

Tribunal Fédéral

PROTECTION DES DONNÉES. AUTODÉTERMINATION EN MATIÈRE DE DONNÉES PERSONNELLES. ENREGISTREMENT CENTRALISÉ DE DONNÉES BIOMÉTRIQUES. NÉCESSITÉ AU REGARD DU PRINCIPE DE LA PROPORTIONNALITÉ. ATTEINTE À LA PERSONNALITÉ. JUSTIFICATION PAR LE CONSENTEMENT DE L'INTÉRESSÉ OU PAR L'INTÉRÊT PRIVÉ PRÉPONDÉRANT DE LA PERSONNE TRAITANT LES DONNÉES. - Mise en service, par un établissement de sports et de détente, d'un nouveau système de contrôle d'accès, basé sur des données biométriques. - Recommandation du Préposé fédéral à la protection des données et à la transparence demandant que l'établissement renonce à l'enregistrement centralisé des données biométriques. - Refus de l'établissement de suivre cette recommandation. - Action ouverte par le Préposé fédéral à la protection des données et à la transparence, admise par le TAF.

Art. 13 al. 2 Cst.; art. 4 al. 2 et 5, art. 12 al. 2 let. a, art. 13 al. 1er LPD.

En vertu de l'art. 4 al. 2 LPD, le traitement de données doit être conforme au principe de la proportionnalité, tant en ce qui concerne son but que ses modalités (c. 3.1).

Il convient de renoncer à une mesure lorsqu'une autre mesure moins incisive permet d'obtenir le résultat escompté (c. 3.3).

Le consentement peut en principe justifier toute atteinte à la personnalité, y compris la violation des principes généraux de protection des données applicables au traitement de données (c. 4.1).

En exigeant que la personne concernée soit dûment informée, la loi veut s'assurer que le consentement est donné en connaissance de cause, c'est-à-dire que la personne concernée ne décide qu'après avoir (aussi) pris connaissance des conséquences négatives que peut entraîner son consentement. Le consentement doit en outre être donné librement. La personne concernée doit disposer d'une "solution de rechange qui ne comporte pas de désavantages inacceptables" (c. 4.2).

Une atteinte à la personnalité n'est pas illicite lorsqu'elle est justifiée par un intérêt privé prépondérant. Dans ce cas, il convient d'établir tant l'intérêt lié au but du traitement de données que l'intérêt lié aux moyens permettant d'atteindre ce but (c. 5).

Les objections soulevées par la personne traitant des données et tirées du principe de la confiance et de l'égalité de traitement par rapport à d'autres systèmes d'accès sont infondées (c. 7).

Après une période d'essai de six mois, les établissements de sports et de détente "KSS Sport- und Freizeitanlagen Schaffhausen" (ci-après: établissements KSS, défendeur) ont introduit en été 2005 un nouveau système de contrôle, afin de lutter contre l'utilisation frauduleuse des cartes d'abonnement nominatives et intransmissibles - semestrielles ou annuelles - donnant accès à la piscine et aux espaces de bien-être. Dans le cadre de ce nouveau système, outre les données personnelles du client - prénom, nom, adresse, langue et date de naissance -, les empreintes digitales de ce dernier sont également relevées puis enregistrées sous forme de gabarit biométrique ("template"), c'est-à-dire de réduction numérisée d'une donnée biométrique brute. Ces données biométriques sont sauvegardées de manière centralisée dans une base de données gérée par les établissements KSS. Le client reçoit une carte équipée d'un transpondeur - au format d'une carte de crédit - assortie d'un identifiant unique. Les données personnelles du client ainsi que le gabarit biométrique sont liés à l'identifiant de la carte. Cependant, la carte ne contient aucune donnée personnelle. Elle est seulement pourvue d'une zone de signature afin qu'on puisse la distinguer visuellement.

Pour pénétrer dans l'établissement, le client doit insérer sa carte d'abonnement dans un lecteur asservissant le tourniquet d'entrée puis faire glisser son doigt sur un scanner. A partir de l'identifiant de la carte, le gabarit biométrique correspondant est extrait de la base de données centralisée puis comparé avec l'empreinte digitale du client. Il s'agit par conséquent d'un processus de vérification. Dans cette mesure, le gabarit d'épreuve de l'empreinte digitale est comparé avec les données de référence, afin d'obtenir la confirmation que la personne en question est bien celle qu'elle prétend être. Toutes les transactions effectuées avec succès sont sauvegardées de manière centralisée avec les données de la carte (la date, l'heure des entrées et sorties ainsi que l'appareil de contrôle ayant procédé à l'enregistrement). Etant donné que toutes les données sont enregistrées de manière centralisée dans une base de données, il est possible, à partir d'un gabarit biométrique, de retrouver la carte d'abonnement correspondante et donc d'identifier la personne concernée.

Le 10 juin 2008, par voie d'action, le Préposé fédéral à la protection des données et à la transparence (ci-après: préposé, demandeur) requiert qu'il soit ordonné aux établissements KSS de renoncer à l'enregistrement *centralisé* des empreintes digitales sous forme de gabarit biométrique et de sauvegarder ces données biométriques - y compris celles qui ont déjà été enregistrées de manière centralisée - sur une carte à puce sécurisée ("smartcard"), qui demeure dans la sphère d'influence de l'utilisateur et sous contrôle de la personne concernée. De cette manière, la vérification de l'identité intervient exclusivement par le biais de ce support de sécurité (comparaison biométrique sur carte, "smartcard match on card"). Ainsi, les données biométriques ne quittent jamais l'environnement sécurisé de ce support et restent sous contrôle de la personne concernée.

Selon le préposé, le traitement de données effectué par les établissements KSS - enregistrement *centralisé* de données biométriques - porte atteinte au droit à l'autodétermination en matière de données personnelles et ne respecte pas le principe de la proportionnalité. La solution qu'il propose porte moins atteinte aux droits fondamentaux des personnes concernées tout en atteignant également le but recherché.

Les établissements KSS concluent au rejet de l'action. Le nouveau système fonctionne parfaitement depuis trois ans et demi. Aucune réclamation n'a été enregistrée. Par ailleurs, les clients ont la possibilité d'acquérir une carte d'abonnement annuelle, sans que leurs données ne soient enregistrées. Certes, cette solution alternative n'a pas été rendue publique. Au demeurant, la recommandation du préposé ne peut pas être mise en œuvre, car elle implique des coûts trop élevés. En outre, ce système est déjà installé dans d'autres établissements de bain et de sports. Enfin, le système utilisé par les remontées mécaniques - stockage centralisé

d'une photographie et enregistrement de chaque passage - constitue une atteinte bien plus grave.

Dans sa réplique, le préposé maintient sa conclusion et ajoute que le traitement de données doit également respecter le principe de la proportionnalité, lorsque la personne concernée a donné son accord et qu'il existe une solution alternative au système de reconnaissance biométrique. Les coûts d'acquisition d'un nouveau système ne sont pas disproportionnés et seront de toute façon répercutés sur les clients. En outre, le préposé a déjà recommandé à de nombreuses reprises l'enregistrement décentralisé des données.

Dans leur duplique, les établissements KSS indiquent qu'il n'est pas possible de répercuter ces nouveaux coûts d'acquisition en raison de la situation économique. En outre, les personnes concernées ont en tout temps la faculté de consulter leurs données; elles n'en perdraient ainsi pas le contrôle. Au demeurant, lors du processus d'acquisition, des systèmes semblables étaient déjà en fonction, sans que le demandeur ne s'y soit opposé. La conclusion du préposé viole par conséquent les principes de la sécurité du droit et de la confiance.

A la demande du TAF, le défendeur indique que le logiciel du système ne permet pas de renoncer à une liste de correspondance. Toujours à la demande du TAF, le préposé expose que l'exemple donné à titre de comparaison - le système d'accès employé par les remontées mécaniques - diffère de la présente cause sur des éléments de fait essentiels. En particulier, l'utilisation de données biométriques ne figurait en aucun cas parmi les faits établis.

Le TAF admet l'action au sens des considérants.

Extrait des considérants:

1. Le préposé établit les faits d'office ou à la demande de tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système, art. 29 al. 1er let. a de la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1)). Après avoir établi les faits, il peut recommander de modifier ou de cesser le traitement conformément à l'art. 29 al. 3 LPD. Si la recommandation est rejetée ou n'est pas suivie, il peut porter l'affaire, par voie d'action, devant le TAF pour décision (art. 29 al. 4 LPD en relation avec l'art. 35 let. b de la loi du 17 juin 2005 sur le Tribunal administratif fédéral (LTAF; RS 173.32)).

1.1 La présente action est dirigée contre le refus, par le défendeur, de suivre une recommandation émise par le préposé, respectivement contre le rejet de cette recommandation. Il s'agit ainsi d'une action au sens de l'art. 29 al. 4 LPD. Il convient en premier lieu de déterminer si la LPD est en l'espèce applicable et si le préposé avait qualité pour agir.

1.2 La LPD régit le traitement de données concernant des personnes physiques et morales effectué par des personnes privées et des organes fédéraux (art. 2 al. 1er LPD).

1.2.1 On entend par données personnelles (données) au sens de l'art. 3 let. a LPD toutes les informations qui se rapportent à une personne identifiée ou identifiable. Il faut comprendre par là toute information qui est conçue pour permettre la transmission ou la conservation d'informations, qu'il s'agisse d'une constatation de faits ou d'un jugement de valeur. Par ailleurs, la forme que prend une affirmation - signe, écrit, image, son ou une combinaison de ces éléments - ainsi que le type de support de données sur lequel sont enregistrées les informations importent peu. Ainsi, une personne est identifiée lorsque l'information à elle seule désigne une personne bien précise (*Urs Belser*, in: Urs Maurer-Lambrou/Nedim Peter Vogt (éd.), Datenschutzgesetz, Basler Kommentar, 2e éd., Bâle 2006, n. 5 s. ad art. 3 LPD). Ce lien avec une personne ne pose pas de problème lorsqu'il résulte de la nature de l'information, comme par exemple les empreintes digitales en matière d'informations biométriques (cf. *David Rosenthal/Yvonne Jöhri*, Handkommentar zum Datenschutzgesetz, Zurich 2008, n. 13 ad art. 3 let. a LPD).

1.2.2 Le défendeur recueille de chaque titulaire d'une carte d'abonnement ses informations personnelles - nom, prénom, adresse, langue et date de naissance. Il s'agit sans aucun doute de données personnelles qui permettent - à elles seules (nom, prénom) ou en lien avec les autres données recueillies (adresse, langue, date de naissance) - d'identifier sans peine une personne. En outre, les empreintes digitales des abonnés sont relevées, afin d'en extraire les minuties, puis transformées, à l'aide d'un algorithme, en un gabarit biométrique, de façon à les sauvegarder dans une banque de données centralisée. L'empreinte digitale, de même que les minuties qui en sont extraites, sont uniques et peuvent être attribuées à une seule personne identifiée. Le lien avec une personne va par conséquent de soi. Le type de support de données (gabarit biométrique) sur lequel sont enregistrées les empreintes digitales importe peu. Au demeurant, une liste de correspondance est également enregistrée de manière centralisée. Elle permet ainsi d'identifier les abonnés.

En conclusion, l'ensemble des données en cause constituent des données personnelles au sens de la LPD.

1.2.3 On entend par traitement au sens de l'art. 2 al. 1er LPD toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données (art. 3 let. e LPD). Le TAF considère qu'il ne fait aucun doute qu'un traitement de données au sens de la LPD est ici en cause. Ceci n'est d'ailleurs pas contesté.

1.2.4 Comme cela a déjà été mentionné, le préposé établit, en vertu de l'art. 29 al. 1er let. a LPD, les faits d'office ou à la demande de tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système). Dans ce contexte, l'"erreur de système" signifie qu'il existe un risque d'atteinte à la personnalité d'un nombre important de personnes (cf. *Rosenthal/Jöhri*, op. cit., n. 11 ad art. 29 LPD; *René Huber*, in: Urs Maurer-Lambrou/Nedim Peter Vogt (éd.), Datenschutzgesetz, Basler Kommentar, 2e éd., Bâle 2006, n. 6 ss ad art. 29 LPD; arrêt rendu par la Commission fédérale de la protection des données le 15 avril 2005, JAAC 69.106 c. 3.2). Lorsque le traitement de données en question risque potentiellement de causer un préjudice à un nombre important de personnes, le seuil limite du "nombre important de personnes" est déjà atteint lorsque quelques cas se sont produits (*Huber*, op. cit., n. 10 s. ad art. 29 LPD). Dans sa réponse, le défendeur indique que 1200 cartes d'abonnement sont vendues annuellement. Par conséquent, on peut considérer sans autre qu'il existe une "erreur de système" au sens de la législation.

1.3 Pour ces motifs, la LPD est applicable et le demandeur avait la compétence d'adresser une recommandation. Il y a par conséquent lieu d'entrer en matière sur l'action, introduite en temps utile et dans les formes requises.

1.4 Conformément à l'art. 44 al. 1er LTAF, la procédure est en principe régie par les art. 3 à 73 et 79 à 85 de la loi fédérale du 4 décembre 1947 sur la procédure civile (PCF; RS 273). Quand bien même, selon cette loi, le juge ne peut fonder son jugement sur d'autres faits que ceux qui ont été allégués dans l'instance (art. 3 al. 2 PCF), en raison de la règle spéciale prévue par l'art. 44 al. 2 LTAF, le TAF établit les faits d'office. (...)

2. 2.1 En premier lieu, le demandeur estime que le système d'accès du défendeur viole le principe de la finalité du traitement de données selon l'art. 4 al. 3 LPD (...). En raison de l'enregistrement centralisé des données biométriques, une modification du but ne pourrait pas être contrôlée par les personnes concernées. Il existe ainsi le risque d'une violation du droit à l'autodétermination en matière de données personnelles prévu par l'art. 13 al. 2 Cst. C'est pourquoi, les données biométriques ne devraient pas quitter la sphère d'influence de la personne concernée. Le préposé recommande par conséquent une mesure moins incisive, appelée "smartcard match on card", permettant une comparaison biométrique sur carte. Les données biométriques seraient enregistrées sur ce support sécurisé et la vérification des données interviendrait également sur la carte.

2.2 La raison pour laquelle le principe de la finalité selon l'art. 4 al. 3 LPD serait en l'espèce violé ne ressort pas du dossier. Le demandeur ne le démontre pas non plus. Il concède d'ailleurs que le défendeur n'a, jusqu'à présent, procédé à aucune modification du but (...). Lorsqu'il se réfère au principe de la *finalité* du traitement de données, le demandeur invoque en fait le principe de la *proportionnalité* du traitement de données, conformément au ch. 2.2 de son mémoire. Il convient par conséquent d'examiner l'action (avant tout) sous cet angle.

3. Selon l'art. 13 al. 2 Cst., toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent. Le législateur a tenu compte de ce droit dans le cadre de la LPD et a assujetti à des règles précises le traitement de données par des personnes privées et par des autorités fédérales (*Ulrich Häfelin/Walter Haller/Helen Keller*, Schweizerisches Bundesstaatsrecht, 7e éd., Zurich/Bâle/Genève 2008, n. 390). Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Personne n'est notamment en droit de traiter des données personnelles en violation des principes définis à l'art. 4 LPD (art. 12 al. 2 let. a LPD).

3.1 Selon l'art. 4 al. 2 LPD, le traitement de données doit être effectué conformément au principe de la proportionnalité. Il doit être conforme au principe de la proportionnalité, tant en ce qui concerne son but que *ses modalités*. Cela implique en premier lieu que des données personnelles ne peuvent être traitées que si ce traitement est objectivement propre à atteindre le but visé et est nécessaire au regard de la fin envisagée. Le principe de la proportionnalité requiert en outre qu'il puisse être raisonnablement exigé de la personne concernée qu'elle tolère le traitement de données, eu égard tant au but poursuivi qu'aux moyens mis en œuvre (principe de la proportionnalité au sens étroit). L'examen du principe de la proportionnalité doit se fonder sur une appréciation de l'ensemble des circonstances (ATF 122 II 193, JdT 1998 I 562), c'est-à-dire également des intérêts de la personne traitant les données (*Rosenthal/Jöhri*, op. cit., n. 19 ss ad art. 4 LPD).

3.2 Selon le ch. 63 de son mémoire, le préposé accepte avec certaines réserves l'introduction du système de reconnaissance biométrique, eu égard au but du traitement. Certes, les mesures introduites par le défendeur ainsi que les traitements de données effectués seraient appropriés pour atteindre le but visé - la lutte contre l'utilisation frauduleuse des cartes d'abonnement - mais ces moyens seraient toutefois disproportionnés compte tenu de l'atteinte portée aux droits fondamentaux de la personne concernée. Le demandeur critique ainsi la nécessité de l'atteinte.

3.3 Il convient de renoncer à une mesure lorsqu'une autre mesure moins incisive permet d'obtenir le résultat escompté. Plusieurs expressions sont utilisées pour désigner la règle de la nécessité d'une mesure: principe de "la nécessité", de "l'atteinte la moins grave possible", de "l'adéquation au but" ou encore "interdiction de prendre des mesures excessives par rapport à l'objectif visé" (*Ulrich Häfelin/Georg Müller/Felix Uhlmann*, Allgemeines Verwaltungsrecht, 5e éd., Zurich/Bâle/Genève 2006, n. 591 s.). L'atteinte ne doit pas aller au-delà de ce qui est nécessaire d'un point de vue matériel, spatial, temporel ou personnel (*Ulrich Häfelin/Walter Haller/Helen Keller*, op. cit., n. 322). Lors de la vérification de l'identité de la personne concernée, les données biométriques doivent être sauvegardées de préférence sur un support d'enregistrement individuel sécurisé - dont l'utilisation peut être contrôlée par la personne concernée - au lieu d'être enregistrées dans une base de données centralisée (*Urs Maurer-Lambrou/ Andrea Steiner*, in: Urs Maurer-Lambrou/Nedim Peter Vogt (éd.), Datenschutzgesetz, Basler Kommentar, 2e éd., Bâle 2006, n. 22 ad art. 4 LPD).

3.4 Dans le cadre du *système actuel*, les données biométriques, accompagnées d'une liste de correspondance, sont enregistrées sur le serveur du défendeur. La carte équipée d'un transpondeur a uniquement pour fonction d'activer le gabarit biométrique correspondant destiné au processus de vérification, afin que le visiteur puisse être identifié en tant qu'abonné grâce à son empreinte digitale. La carte ne contient aucune donnée. Le processus de vérification intervient sur le serveur. Chaque transaction effectuée avec succès est enregistrée.

3.5 Dans le cadre du *système recommandé* par le demandeur, intitulé "smartcard match on card", la comparaison entre les caractéristiques biométriques (empreinte digitale) et les données biométriques sauvegardées localement (gabarit biométrique de référence) est réalisée de manière décentralisée sur la carte. De cette façon, le serveur reçoit uniquement un signal de validation de la carte à puce. Aucune donnée biométrique n'est échangée entre la carte à puce et le système électronique de contrôle d'accès. Ainsi, les personnes concernées gardent le contrôle sur leurs données biométriques de référence ainsi que sur les données de transaction relatives au processus de comparaison. Dans un tel cas de figure, seules les données de transaction échangées entre la carte à puce et le lecteur ne se trouvent pas sous le contrôle de la personne concernée.

3.6 En comparant ces deux différents systèmes d'accès, force est de constater que le système exigé par le demandeur porte beaucoup moins atteinte - par rapport au système utilisé jusqu'à présent - au droit à l'autodétermination de la personne concernée en matière de données personnelles et que le but recherché peut quand même être atteint. La personne concernée ne cède plus ses données et en garde par conséquent toujours le contrôle. Le fait que l'abonné puisse consulter en tout temps ses données dans le cadre du système d'accès en cause - comme l'invoque le défendeur - ne permet de loin pas d'obtenir les possibilités de contrôle offertes par le système d'accès recommandé par le demandeur. Les données enregistrées de manière centralisée, hors de la sphère d'influence de l'abonné, demeurent majoritairement inaccessibles à son endroit et portent ainsi atteinte à ses droits.

3.7 En lien avec l'art. 36 al. 4 let. c LPD, qui permet au Conseil fédéral d'édicter des dispositions concernant le mode selon lequel les moyens d'identification de personnes peuvent être utilisés, le commentaire de la LPD précité se réfère au rapport final du demandeur du 11 avril 2006 et soutient ainsi la présente conclusion exigeant un enregistrement décentralisé des

données biométriques (cf. *Rosenthal/Jöhri*, op. cit., n. 35 s. ad art. 36 al. 4 let. c LPD). Dans le cadre de son 11e rapport d'activités 2005, le préposé zurichois à la protection des données a également recommandé de recourir, de préférence, à des systèmes qui ne sauvegardent pas les données biométriques auprès de l'exploitant d'une piscine (...). Le groupe de travail "article 29", organe consultatif indépendant de l'Union européenne en matière de protection des données, s'est également prononcé en ce sens. Ainsi, lorsque des données biométriques sont utilisées pour contrôler un accès, elles ne doivent pas être enregistrées sur un support qui n'est pas possédé par la personne concernée (cf. le document du groupe de travail "article 29" sur la biométrie, 1er août 2003, ch. 3.2, p. 7). Les pays européens ont suivi cette recommandation - en particulier l'Italie et la France - et se prononcent également en faveur d'un enregistrement décentralisé, comme le requiert le demandeur. De son côté, le demandeur a déjà pris position dans un cas (semblable) qui concernait l'enregistrement et l'embarquement à l'aéroport de Zurich. Les empreintes digitales des passagers étaient relevées puis enregistrées sous forme de gabarit biométrique. Le préposé a alors également recommandé l'enregistrement décentralisé (...).

3.8 Au demeurant, le défendeur a, par lettre du 10 août 2006, approuvé la recommandation n° 2 - soit la conclusion du demandeur - (...) et affirmé que les cartes d'abonnements seraient remplacées par des supports inscriptibles. Le logiciel serait adapté de manière à ce que les données puissent être enregistrées sur la carte. En outre, il ressort de la lettre du 29 février 2008 que le défendeur invoque uniquement les coûts élevés d'acquisition et les frais supplémentaires en matière de logistique pour continuer à enregistrer les données de manière centralisée. En revanche, il ne défend pas le point de vue que le système d'accès requis par le demandeur ne constituerait pas une mesure moins incisive au sens de la proportionnalité. Cette position peut s'expliquer, dans la mesure où il n'existe visiblement aucun motif pouvant justifier la nécessité d'enregistrer les données de manière centralisée. D'ailleurs, le défendeur ne le prétend pas.

3.9 Pour ces motifs, l'enregistrement centralisé des données biométriques, tel qu'il a été mis en œuvre par le défendeur jusqu'à maintenant, est en contradiction avec la règle de la nécessité et viole par conséquent le principe de la proportionnalité du traitement de données prévu par l'art. 4 al. 2 LPD. Il existe ainsi une atteinte à la personnalité au sens de l'art. 12 al. 2 let. a LPD.

4. Toute atteinte à la personnalité n'est pas forcément illicite. L'illicéité constitue seulement le principe, pour lequel il existe des exceptions. Ainsi, une atteinte à la personnalité n'est pas illicite lorsqu'elle est justifiée, entre autres, par le consentement de la victime (art. 13 al. 1er LPD).

4.1 Le *consentement* peut en principe justifier toute atteinte à la personnalité, y compris la violation des principes généraux de protection des données applicables au traitement de données (cf. *Corrado Rampini*, in: Urs Maurer-Lambrou/Nedim Peter Vogt (éd.), Datenschutzgesetz, Basler Kommentar, 2e éd., Bâle 2006, n. 3 s. ad art. 13 LPD). Pour définir la notion de consentement, le législateur s'est inspiré de la notion de consentement éclairé du patient (cf. ATF 119 II 456, en fr., rés. JdT 1995 I 29; ATF 117 Ib 197, JdT 1992 I 214; ATF 114 Ia 350, en fr.), dans le sens où la personne concernée doit disposer de tous les éléments du cas d'espèce qui lui permettent de prendre librement sa décision (Message du Conseil fédéral du 19 février 2003 relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, FF 2003 1939). Pour que le consentement soit juridiquement valable en vertu de l'art. 4 al. 5 LPD, la personne concernée doit avoir été dûment informée du traitement de données auquel elle consent et elle doit avoir exprimé librement sa volonté d'accepter le traitement de données (*Rosenthal/Jöhri*, op. cit., n. 67 s. ad art. 4 al. 5 LPD).

4.2 En exigeant que la personne concernée soit *dûment informée*, la loi veut s'assurer que le consentement est donné en connaissance de cause, c'est-à-dire que la personne concernée ne décide qu'après avoir (aussi) pris connaissance des conséquences négatives que peut entraîner son consentement. Il faut - ce qui par ailleurs suffit également - que la personne concernée soit au clair sur ce à quoi elle consent, c'est-à-dire qu'elle ait conscience de la portée de sa décision. Suivant les circonstances, il sera nécessaire d'obtenir des renseignements non seulement au sujet des modalités du traitement de données, mais également à propos des principaux risques et conséquences pour la personne concernée, en particulier lorsqu'ils sont très sérieux. La question de savoir si et dans quelle mesure la personne concernée doit être informée dépend au final des circonstances concrètes (*Rosenthal/Jöhri*, op. cit., n. 72 s. ad art. 4 al. 5 LPD). Le consentement doit être donné *librement*, c'est-à-dire qu'il doit être l'expression de la libre volonté de la personne concernée. Le consentement obtenu par tromperie, sous la menace ou la contrainte, n'est pas valable. La personne concernée doit disposer d'une "solution de rechange qui ne comporte pas de désavantages inacceptables" (*Rampini*, op. cit., n. 6 s. ad art. 13 LPD; cf. également *Christian Drechsler*, Die Revision des Datenschutzrechts, in: PJA 2007 p. 1473). Dans le commentaire de la

LPD précité, *David Rosenthal* a une opinion quelque peu divergente et estime que cela est excessif: lorsque l'on peut partir du principe que le consentement est subjectivement dans l'intérêt de la personne concernée, on peut normalement considérer que celle-ci a exprimé librement sa volonté, même si elle ne dispose pas d'une solution de rechange. Cependant, sa critique ne concerne pas la présente cause, étant donné que le consentement n'apporte aucun avantage à la personne concernée et qu'il n'est pas dans son intérêt d'un point de vue subjectif.

4.3 Le défendeur invoque comme motif justificatif le consentement, en expliquant que les personnes concernées sont rendues attentives, lors de l'achat d'une carte d'abonnement, au système de contrôle et au traitement de données. Cependant, la solution alternative, soit la délivrance d'une carte d'abonnement sans que les empreintes ne soient relevées, n'est pas rendue publique. Elle est proposée au client seulement à partir du moment où il refuse de donner ses empreintes. Enfin, les personnes concernées auraient en tout temps la possibilité de consulter leurs données.

4.4 Dans son rapport final, le demandeur expose à propos du consentement de la personne concernée qu'il n'existe aucune solution alternative. Les clients doivent en effet se rabattre sur des abonnements à 10 entrées bien plus onéreux. Par ailleurs, lors du renouvellement ou de l'acquisition d'une carte d'abonnement, les baigneurs seraient informés par oral, par le personnel à la caisse, de la collecte des données biométriques et du traitement subséquent de ces données. Lors de l'établissement des faits sur place, aucun feuillet explicatif n'aurait été disponible sur le comptoir de la caisse. Selon le préposé, le feuillet explicatif a pu être fourni seulement après une petite recherche. Il est intitulé: "La protection des données est-elle garantie lors de la reconnaissance et de l'identification biométrique de l'empreinte digitale?". Le feuillet indique que les données biométriques brutes ne sont pas enregistrées, mais que les caractéristiques extraites d'une empreinte digitale sont sauvegardées dans la base de données sous forme d'un gabarit biométrique "codé". Le dépliant explique ensuite comment se passe la

comparaison avec le gabarit biométrique et qu'il n'est pas possible de reconstruire, à partir du "code", les données biométriques brutes. Il est enfin mentionné que les bases de données sur des personnes, aujourd'hui fréquentes, présenteraient un danger bien plus grand, d'un point de vue de la protection des données, que les données extraites d'une empreinte digitale. Le feuillet explicatif décrit uniquement d'une manière générale les modalités de traitement des données recueillies. Il explique avant tout les raisons pour lesquelles le fournisseur du système considère que le recours à la biométrie ne pose aucun problème.

Dans sa proposition d'amélioration n° 1, le demandeur suggère d'augmenter fortement le contenu informatif du dépliant à propos des modalités de traitement des données biométriques. Les éléments principaux du traitement de données doivent être énumérés: il s'agit notamment d'indiquer l'endroit où sont sauvegardées les données ainsi que la durée prévue de l'enregistrement. Il convient également d'expliquer ce qu'il advient des gabarits biométriques et des données de transaction, de mentionner le cercle de personnes ayant accès aux données ainsi que les personnes auxquelles ces données pourraient être transmises - si tant est qu'elles le soient. Le personnel à la caisse doit automatiquement remettre à chaque client le dépliant, et ce avant que les données ne soient enregistrées. Le baigneur doit avoir assez de temps à disposition pour la lecture du dépliant. Des feuillets supplémentaires doivent se trouver à portée de main sur le comptoir de la caisse. Par lettre du 18 octobre 2006, le défendeur a accepté cette proposition d'amélioration et a indiqué qu'elle serait mise en œuvre. Le dépliant sera complètement remanié et les points énumérés par le demandeur seront pris en compte. En outre, le personnel à la caisse recevra un schéma détaillant la manière de procéder lors de la délivrance d'un abonnement (avec des données biométriques). Il ne ressort pas du présent dossier que le défendeur a effectivement mis en œuvre la proposition d'amélioration.

4.5 L'opinion du demandeur doit être suivie: le baigneur n'a (concrètement) aucune solution alternative, s'il obtient la possibilité d'acquérir un abonnement semestriel ou annuel sans que ses empreintes digitales ne soient relevées, seulement à partir du moment où il a refusé d'acheter la carte d'abonnement fonctionnant avec le système d'accès actuel. Dans la plupart des cas, le client se laissera convaincre, (prétendument) faute d'alternative, et acceptera que ses données biométriques soient enregistrées de manière centralisée. Par conséquent, on ne peut pas considérer que le client exprime librement sa volonté.

4.6 Au demeurant, le client n'est pas non plus dûment informé, ce qui lui permettrait d'avoir (complètement) conscience de la portée de sa décision. Dans un premier temps, le feuillet explicatif ne lui est manifestement même pas remis. Si, lors de l'inspection locale, le dépliant n'a pu être donné qu'après une petite recherche, alors même que l'enquête menée sur place par le préposé avait été convenue à l'avance, on ne peut pas partir du principe que, dans des "circonstances normales", le feuillet explicatif sera toujours à portée de main sur le comptoir, et encore moins qu'il sera distribué. En outre, le personnel à la caisse semble n'avoir reçu aucune instruction et formation spécifiques concernant la procédure à suivre lors de la vente d'une carte d'abonnement. Par conséquent, le défendeur n'informe pas dûment le client, comme cela est requis par la loi.

Partant, le TAF n'a pas besoin de se prononcer sur le contenu du dépliant ni d'examiner si les explications données suffisent. Il convient uniquement de mentionner que les données biométriques constituent (incontestablement) des données sensibles et que l'information fournie à ce propos devrait être complète. Cependant, au vu de la description incontestée, faite par le demandeur, du contenu du dépliant et de la proposition d'amélioration, force est de constater que le dépliant n'informe pas de manière suffisante.

5. Une atteinte à la personnalité n'est pas illicite lorsqu'elle est justifiée par un *intérêt privé prépondérant* (art. 13 al. 1er LPD). S'agissant de la personne qui traite les données, il convient de prendre uniquement en considération les intérêts privés justifiant le traitement de données. Dans ce cas, il s'agit d'établir tant l'intérêt lié au but du traitement de données que l'intérêt lié aux moyens permettant d'atteindre ce but. Les moyens comprennent notamment les modalités du traitement de données et le choix des données personnelles (*Rosenthal/Jöhri*, op. cit., n. 8 ad art. 13 al. 1er LPD).

5.1 Le défendeur fait valoir dans ce contexte que les modifications exigées par le demandeur entraîneraient des coûts élevés d'acquisition et des frais supplémentaires en matière de logistique.

5.2 En revanche, le demandeur considère qu'il est de la responsabilité du maître du fichier de veiller à ce qu'une installation soit dès le départ conforme à la protection des données. Par conséquent, les coûts occasionnés par la modification du système ainsi que les frais supplémentaires en matière de logistique ne constituent pas des arguments pertinents.

5.3 Il convient en l'espèce de ne pas prendre en considération les intérêts du défendeur, car ceux-ci ne se rapportent pas au traitement de données, mais se fondent uniquement sur les désagréments qui seraient causés par une éventuelle modification du système conformément à la conclusion du demandeur. Ces intérêts n'ont aucun poids en tant que motif justificatif au sens de l'art. 13 al. 1er LPD. Il n'existe ainsi aucun motif justifiant le comportement du défendeur.

6. En résumé, dans le cadre du système d'accès en cause et des modalités du traitement des données biométriques, le défendeur viole le principe de la proportionnalité. Cette atteinte à la personnalité n'est justifiée ni par un consentement ni par un intérêt privé prépondérant. Par conséquent, la question de savoir s'il existe également un danger que les données soient exportées, copiées ou qu'elles fassent l'objet d'un traitement subséquent non autorisé - comme le prétend le demandeur qui estime que la sécurité des données n'est pas garantie au sens de l'art. 7 LPD - peut rester ouverte.

Il appartient au TAF d'établir si un système d'accès est conforme à la protection des données. En revanche, il ne lui appartient pas de déterminer les modalités du traitement lors de l'utilisation de données biométriques et de livrer ainsi un système d'accès complet (respectant la protection des données). Cependant, à première vue, le système proposé par le demandeur semble être adéquat et permet de respecter les exigences légales en matière de traitement des données biométriques. Dans le cadre de l'examen de la proportionnalité, il constitue en tout cas une mesure moins incisive au regard du principe de la nécessité. Etant donné que, pour des raisons techniques, la liste de correspondance ne peut pas être supprimée de la base de données et qu'il n'est ainsi pas possible de séparer cette liste des gabarits biométriques correspondants (...), aucune mesure moins incisive pour le défendeur ne peut être présentée dans le cadre de la présente procédure. Afin de contrôler si une personne a le droit d'entrer, il serait peut-être suffisant de sauvegarder les gabarits biométriques sans liste de correspondance et, lors du contrôle à l'entrée, d'examiner uniquement si l'empreinte présentée figure dans la base de données. Au moins, dans le cadre de telles procédures de comparaison automatique des données ("matching"), le personnel chargé de l'enregistrement des données n'aurait pas la possibilité d'établir un lien avec une personne déterminée, à condition que la base de données soit suffisamment grande (*Gerrit Hornung*, Der Personenbezug biometrischer Daten, in: Datenschutz und Datensicherheit, 28 (2004) 7, p. 430).

Le défendeur est cependant libre de renoncer de lui-même à utiliser un système biométrique. Il n'existe aucun motif pour imposer au défendeur un autre système d'accès.

7. On ne peut pas non plus suivre le défendeur lorsqu'il prétend que la manière d'agir du demandeur viole le principe de l'égalité de traitement et celui de la confiance, parce que le système de contrôle des remontées mécaniques, par exemple, ne fait pas l'objet de critiques et que le demandeur n'a émis aucune objection pendant le processus d'acquisition, alors même que des systèmes semblables auraient déjà été utilisés.

7.1.1 Le principe de la confiance (art. 9 Cst.) confère à l'administré le droit d'être protégé dans la confiance légitime qu'il met dans les assurances reçues de l'autorité ou dans tout autre comportement de sa part fondant des attentes précises (*Häfelin/Müller/ Uhlmann*, op. cit., n. 627). Pour que l'on puisse invoquer le principe de la confiance, la présence d'éléments susceptibles de créer la confiance de l'administré est, entre autres, requise. Le degré de précision de ces éléments est décisif. Ils doivent être précis au point que l'administré puisse en retirer les informations déterminantes pour prendre des dispositions (*Häfelin/Müller/Uhlmann*, op. cit., n. 631). La tolérance passagère d'une situation illicite n'empêche en principe pas l'autorité de corriger par la suite cette situation. L'inactivité d'une autorité crée seulement dans des cas exceptionnels un lien de confiance qui s'oppose, totalement ou partiellement, au rétablissement d'une situation conforme au droit (*Häfelin/ Müller/Uhlmann*, op. cit., n. 652). En l'espèce, le défendeur ne peut pas s'appuyer sur des éléments suffisants susceptibles de créer la confiance, comme par exemple une assurance écrite ou orale du demandeur. Il ne peut pas non plus invoquer, conformément au principe de la confiance, que des systèmes semblables - à la rigueur également non conformes à la législation en matière de protection des données - auraient déjà été utilisés et que le demandeur n'aurait pas pris des mesures. Aucune exception n'a manifestement été faite sur ce point; le défendeur ne le prétend d'ailleurs pas.

7.1.2 Le défendeur ne peut pas non plus se fonder sur le principe de l'égalité de traitement. Le droit à l'égalité de traitement exige que les droits et obligations des personnes concernées soient déterminés selon le même critère. Il convient de traiter de la même manière les situations semblables en fonction de leur similitude et différemment les situations différentes en fonction de leur différence. Le principe de l'égalité interdit d'une part d'édicter des réglementations différentes qui ne reposent pas sur des différences juridiques importantes. D'autre part, ce principe proscrit également que des situations, dont les éléments de fait se distinguent de manière importante, soient juridiquement traitées de manière égale. Le principe de l'égalité de traitement impose au législateur comme à l'autorité administrative de traiter de la même manière deux situations non pas à la condition qu'elles soient en tous points parfaitement identiques, mais lorsque leur similitude réside dans les éléments de fait qui sont pertinents pour la norme à adopter ou pour la décision à prendre (*Häfelin/Müller/Uhlmann*, op. cit., n. 495). En cas de conflit, le principe de la légalité de l'activité administrative l'emporte, en règle générale, sur celui de l'égalité. Lorsqu'une autorité a, dans un cas concret, rendu une décision qui déroge à la loi, on ne saurait en déduire un droit, pour le justiciable qui se trouve dans une situation identique, d'obtenir une décision qui déroge également à cette norme légale (*pas d'égalité dans l'illégalité*). Cependant, cela vaut uniquement lorsque le traitement illégal s'est produit dans un ou quelques cas isolés. En revanche, lorsqu'il existe une pratique constante et que l'autorité refuse de l'abandonner, l'administré peut exiger qu'on lui octroie également l'avantage illicite accordé à des tiers (arrêt du TAF A-5541/2008 du 2 juillet 2009, c. 5.1 et les réf.; *Häfelin/Müller/Uhlmann*, op. cit., n. 518). Le système d'accès des remontées mécaniques, auquel le défendeur fait appel à titre de comparaison, présente d'importantes différences par rapport au système d'accès en question. Comme le démontre le demandeur, dans le cadre du système d'accès des remontées mécaniques, les données biométriques ne faisaient absolument pas partie des faits établis. Cela indique que de telles données ne sont manifestement pas utilisées. Ainsi, les éléments de fait pertinents sont différents et ne permettent pas de procéder à une comparaison. En outre, le demandeur a l'intention d'appliquer la jurisprudence, une fois qu'elle aura été établie, à tout traitement similaire de données biométriques dans n'importe quel domaine, afin de favoriser l'émergence d'une pratique uniforme.

8. Pour ces motifs, il convient d'admettre l'action au sens des considérants.

Trad. Laurent Butticaz