

3 - LES ENJEUX DE LA BIOMETRIE EN 2003

Claudine Guerrier

La biométrie connaît une expansion spectaculaire : de 47 millions d'euros en 1999, le marché est passé, selon l'International Biometric Group, à 600 millions d'euros en 2003. En effet, elle apparaît, tant aux acteurs privés que publics, comme une parade contre les dangers multiformes.

Selon le *Petit Robert*, la biométrie est « la science qui étudie, à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé ». Pratiquement, la biométrie permet l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissables et vérifiables. La biométrie morphologique identifie les traits physiques qui sont uniques, permanents pour chaque individu ; elle distingue la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'œil. La biométrie comportementale identifie certains comportements d'une personne physique comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier. Les autorités de régulation, telles la Commission d'accès à l'information au Québec et la Commission nationale de l'informatique et des libertés (CNIL) en France reprennent ces distinctions auxquelles elles ont ajouté l'analyse de l'ADN, du sang et des odeurs. La recherche débouche sur de nouveaux types biométriques comme la forme de l'oreille et la thermographie faciale.

Les techniques biométriques existent depuis longtemps. Les empreintes digitales ont été exploitées dès le dix-neuvième siècle par l'institution policière. Au vingt-et-unième siècle, avec l'expansion de l'idéologie, de l'économie et du droit sécuritaires, la biométrie devient un marché porteur. Mais l'image de la biométrie est ambivalente. Adjointe à l'efficacité policière, elle est pourfendeuse de délits et de crimes, elle est le meilleur défenseur de la société civile. Placée dans un contexte politique délétère, elle est le suppôt et le support des régimes totalitaires. Dans *Le deuxième cercle*¹ de Soljenitsyne, l'utilisation de la reconnaissance vocale brise des vies et devient un outil de répression au service de Staline.

En 2003, la biométrie met l'accent sur deux enjeux principaux : le contrôle des flux migratoires et la protection des données personnelles.

Le contrôle des flux migratoires

Le contrôle des flux migratoires est un souci pour tous les pays occidentaux où l'immigration est importante. L'identification des personnes physiques qui entrent sur le sol d'un

¹ Publié chez Laffont en 1966

Etat étranger n'est pas toujours évidente. Officiellement, vient s'ajouter la crainte d'une menace terroriste venue de l'étranger : ceci correspond à la position des USA.

Le contrôle des flux migratoires implique un statut, au regard de la biométrie, du droit d'asile, des passeports et des visas ainsi que des cartes d'identité.

Le principe de la libre circulation des personnes est mentionné dans le traité de Rome, de même que la libre circulation des marchandises. Le traité d'Amsterdam pose les bases de cette libre circulation. Les personnes étrangères à l'Union européenne peuvent demander le droit d'asile aux pays de cette dernière qui sont des démocraties et qui doivent protéger les personnes persécutées dans leur Etat d'origine.

Le droit d'asile

Dans l'Union européenne, les fondements de la limitation du droit d'asile sont la Convention de Dublin et le règlement du 11 décembre 2000.

La Convention de Dublin du 15 juin 1990, complétée par le règlement du Conseil du 18 février 2003 est applicable depuis 1997. Il s'agit d'éviter l'entrée irrégulière d'étrangers sur le territoire de l'Union européenne. En raison des fraudes possibles, les ministres en charge de l'immigration établissent, à l'échelle européenne, un projet visant à comparer les empreintes digitales des demandeurs d'asile.

Le règlement du 11 décembre 2000 permet de stocker les empreintes digitales des demandeurs d'asile. Par deux avis des 7 juillet et 21 septembre 2000, le Parlement européen s'était opposé à l'enregistrement des empreintes digitales des mineurs. Le Conseil a passé outre. Les données enregistrées sont les empreintes digitales, l'Etat d'où le demandeur d'asile est originaire, le sexe, le numéro de référence. Elles sont conservées pendant dix ans, sauf si le demandeur d'asile obtient la citoyenneté d'un pays de l'Union européenne.

Un autre règlement 407/2002, destiné à la mise en application du précédent règlement a été adopté par le Conseil et le Parlement. Il est en phase avec le système Eurodac, qui est entré en vigueur dans l'Union européenne le 15 janvier 2003. Ce dernier comprend un système central d'identification des empreintes digitales des demandeurs d'asile et, dans seize pays européens, un système de transmission électronique des empreintes digitales dont l'objectif est de lutter contre l'immigration clandestine. En effet, avec Eurodac, les Etats-membres peuvent identifier les demandeurs d'asile et les personnes qui franchissent irrégulièrement une frontière extérieure de la Communauté. Après comparaison des empreintes, les Etats sont susceptibles de savoir si un demandeur d'asile ou un ressortissant étranger en situation illégale a déjà formulé une demande dans un autre Etat de l'Union européenne. La finalité est de combattre les demandes d'asile multiples. L'unité centrale de comparaison d'empreintes digitales est gérée par la Commission européenne. La base de données informatisée, les moyens électroniques de transmission sécurisée entre les Etats et la base de données centrale complètent Eurodac. Le numéro de référence relie l'empreinte digitale à une personne physique et identifie l'Etat-membre qui a envoyé les données.

Eurodac a d'abord été testé au Royaume-Uni. Les étrangers demandeurs d'asile politique ont expérimenté des cartes à puce qui contenaient leurs empreintes digitales fournies par le ministère de l'Intérieur. Une carte d'identité (*Application Registration Card*) est remise au demandeur d'asile ; elle comprend les empreintes digitales, une photo, le nom patronymique, la date de naissance et la nationalité d'origine.

Ces dispositions, depuis l'adoption des règlements et d'Eurodac, s'appliquent à toute personne âgée de quatorze ans et plus. Elles concernent les Etats de l'Union européenne, et trois Etats tiers qui se sont engagés à introduire Eurodac sur leur territoire : la Norvège, l'Islande et la Suisse. La biométrie, via les empreintes digitales, est généralisée dans la politique d'asile.

Passeports et visas

Le G8 (les sept pays les plus industrialisés, auxquels s'adjoint la Russie) a décidé, en mai 2003, de choisir pour les passeports et les visas le procédé biométrique le plus approprié. Un groupe d'experts est constitué pour proposer une solution adéquate. Cette procédure présente un certain caractère d'urgence puisque les USA ont décidé d'exiger des étrangers des passeports utilisant les techniques biométriques. La France est plutôt favorable à l'utilisation des empreintes digitales. Cependant, d'autres choix sont possibles : l'Allemagne préfère la reconnaissance par l'iris, les USA utilisent surtout les empreintes digitales et la reconnaissance faciale, même si cette dernière semble moins efficace. D'ici peu de temps, les déplacements dans les Etats du G8 impliqueront le recours à des visas et des passeports biométriques. Cette solution est critiquée par certaines associations de défense des droits de l'homme qui mettent l'accent sur le danger d'atteinte aux libertés individuelles. En effet, la liberté de circulation, non seulement pour les marchandises, mais pour les personnes physiques, est un principe de base adopté et défendu par les démocraties. Les défenseurs des visas et des passeports biométriques arguent que l'identification biométrique n'est pas une atteinte portée à la liberté de circulation, mais simplement une mesure de maîtrise destinée à empêcher d'éventuels ennemis de la liberté de nuire aux pays démocratiques.

La carte d'identité

Il n'y a pas d'unicité en la matière et l'utilisation de la biométrie a relancé le débat. En Europe, les situations sont différentes selon les Etats. La carte nationale d'identité existe dans tous les pays de l'Union européenne, sauf au Danemark et au Royaume-Uni. A l'exception de l'Italie et de la France, la détention de la carte d'identité est obligatoire. En France, la détention était obligatoire avant 1955. Depuis, la détention d'une carte d'identité est facultative, mais la grande majorité des Français en ont une. Le décret français du 19 mars 1987 a institué une carte d'identité sécurisée ; sa délivrance est généralisée depuis décembre 1995. Etablie sur un papier spécial plastifié, elle comprend plusieurs dispositifs de sécurité destinés à empêcher la falsification. Les techniques biométriques en matière de cartes nationales d'identité sont utilisées en Espagne, en Italie, au Portugal, en France. La prise des empreintes digitales en Italie est obligatoire depuis peu ;

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

elle est appliquée depuis octobre 2002. En France, lors de la constitution de dossier d'une demande, a lieu un relevé des empreintes digitales de la personne concernée. Les enfants de moins de treize ans sont exemptés de cette procédure.

L'Union européenne se dirige vers une généralisation des cartes d'identité nationales. Au Royaume-Uni, la création d'une nouvelle carte d'identité est vivement discutée. La carte d'identité nationale a déjà prévalu lors des deux guerres mondiales du vingtième siècle, pour combattre les ennemis de l'intérieur et de l'extérieur mais elle fut supprimée en 1952. Le 3 juillet 2002, le ministre de l'intérieur a proposé l'introduction d'une carte d'identité, qui aurait pour mission la suppression de la fraude aux documents d'identité, la lutte contre l'immigration clandestine et le travail clandestin. Cette carte permettrait aussi un meilleur accès aux services publics de santé et d'éducation. Les techniques biométriques étudiées sont les empreintes digitales et l'iris. Le gouvernement souhaite obtenir l'agrément de la société civile. En effet, une initiative précédente n'avait pas remporté l'adhésion. De plus, l'introduction d'une nouvelle carte d'identité aurait pour conséquence l'amendement de l'*Human Rights Act*. Une consultation publique a eu lieu au cours du second semestre 2002 et s'est poursuivie jusqu'au 31 janvier 2003.

En Suisse, qui n'est pas membre de l'Union européenne, mais qui est un pays européen, susceptible à moyen terme d'adhérer à l'Union européenne, l'autorité de régulation en matière de protection des données personnelles manifeste ses réserves à l'égard de l'utilisation des techniques biométriques dans les documents d'identité. Le Préposé fédéral à la protection des données est hostile à un processus de surveillance généralisée, telle qu'elle est apparue dans d'autres pays occidentaux sous couvert de lutte contre le terrorisme. Le Préposé demande que, en matière de documents d'identité, les techniques biométriques soient utilisées avec prudence. Il convient d'exclure au moins les données sensibles, notamment concernant la santé.

Au Canada, le ministère fédéral de la citoyenneté et de l'immigration envisage de rendre obligatoire une carte d'identité avec indications biométriques. Un débat public s'est instauré. La Commission d'accès à l'information du Québec a fait part de ses réticences. La mise en place d'une carte d'identité implique la création de banques de données regroupant des informations sur l'ensemble de la population.

A Ottawa, la carte d'identité nationale s'inscrit dans le cadre d'une politique de sécurité. Les relations privilégiées entre le Canada et les USA ont joué un rôle dans le projet de création d'une carte d'identité. Cette dernière faciliterait les vérifications douanières et permettrait un meilleur contrôle des frontières. Selon le ministre canadien de la citoyenneté et de l'immigration, une carte canadienne biométrique pourrait éviter aux Canadiens d'être fichés aux USA.

Le Comité permanent de la citoyenneté et de l'immigration a rendu ses conclusions à l'automne 2003 et un forum national est s'instauré. La carte d'identité comprendrait des empreintes digitales ou la reproduction d'un iris. L'adoption d'une carte d'identité biométrique permettrait de lutter contre les vols d'identité et les vols d'adresses. Néanmoins, des obstacles ou des critiques apparaissent. L'état civil est jusqu'à présent l'apanage des provinces, ce qui rendrait indispensable

une réforme constitutionnelle. Par ailleurs, le coût de la mesure est élevé. Enfin, la carte est considérée par le Commissaire à la protection de la vie privée comme une menace contre les libertés publiques.

Le contrôle des flux migratoires est cependant l'apanage de la biométrie.

La protection des données personnelles

La biométrie entretient des rapports ambivalents avec la protection des données personnelles : sont pris en compte le principe de proportionnalité en matière de sécurité, les diverses techniques biométriques, les relations entre biométrie et droit du travail.

De nombreux pays ont adopté des lois afférentes à la protection des données personnelles sous l'impulsion des lignes directrices de l'OCDE (septembre 1980). Quant à l'Union européenne et au Québec, ils sont très protecteurs en la matière.

Au sein de l'Union européenne, les directives sur la protection des données personnelles, notamment dans le secteur des télécommunications, puis des communications électroniques ont pour fil conducteur le respect de la vie privée. Elles s'appliquent aux personnes physiques identifiées ou identifiables. La personne identifiable peut être reconnue par des éléments spécifiques, propres à son identité physique, physiologique. Si le terme « biométrie » n'apparaît pas dans les textes, il est visé, sans aucun doute, par les directives : les usages biométriques sont en relation étroite, constante, avec l'identité physique et physiologique des personnes. Des procédés biométriques peuvent être considérés comme inconciliables avec les directives. Le recours à certaines applications biométriques peut présenter un caractère excessif et disproportionné par rapport à la finalité du traitement.

Le Québec, en matière de protection des données nominatives informatisées a devancé l'Union européenne. Ses lois trouvent leur origine dans la charte des droits et libertés de la personne, de 1975. La loi sur la protection des renseignements personnels dans le secteur privé fut adoptée en 1994. En 2001, des mesures législatives ont été prises dans le cadre des technologies de l'information. Les données biométriques sont considérées comme des identifiants.

Le principe de proportionnalité en matière de sécurité

En matière de protection de sites ou d'opérations sensibles en France, la Commission nationale de l'informatique et des libertés applique le principe de proportionnalité qui dit que toute limitation d'une liberté doit être proportionnée au danger encouru.

Ainsi elle a émis un avis favorable à la suite d'une demande formulé par l'établissement de la Hague de la Cogema², tendant à installer un lecteur d'empreintes digitales à l'attention du personnel et des visiteurs. En effet, le stockage de matières nucléaires n'est pas inoffensif et doit

² Compagnie générale des matières nucléaires

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

être contrôlé. Certaines zones sont sous secret défense. L'institution d'une banque de données d'empreintes digitales se justifie.

Dans le transport aérien, c'est aussi le cas pour les aéroports, qui reçoivent un vaste public et où il est possible de commettre des actes de terrorisme. Certaines zones sont jugées plus sensibles. A Roissy et à Orly, a été expérimenté un contrôle des « zones réservées sûreté » : cela affecte l'accès des personnels des aéroports de Paris, des services publics et des entreprises qui interviennent dans ces zones. Cette expérimentation utilise soit les empreintes digitales, soit la reconnaissance palmaire, soit l'iris. Pendant l'expérimentation, le stockage a lieu sur une base de données centralisée. A terme, est prévu un stockage sur carte à puce. L'usage de la biométrie est généralisé d'ici la fin 2003 pour le contrôle des personnels, travaillant en zone réservée, puis étendu aux passagers.

Cela peut concerner également certains vols : Air France a testé, avec l'accord de la CNIL, une technique biométrique utilisant les empreintes digitales au départ de vols à destination de Tel Aviv. Il convient de s'assurer que le client d'Air France ayant fait enregistrer un bagage est bien la personne qui embarque dans l'avion. L'empreinte digitale est relevée par le biais d'un boîtier électronique installé sur le comptoir d'enregistrement, puis comparée avec un boîtier similaire au moment de l'accès à bord. La CNIL, dans son avis favorable, a exigé le respect de la confidentialité des informations.

La biométrie dans les prisons est utilisée aux USA comme en Europe. Elle a pour finalité de renforcer la surveillance, à l'occasion de l'accès et lors du retour du parloir. En France, une expérimentation a eu lieu à la prison de la Santé, avec l'avis favorable de la CNIL. Un arrêté du 26 juin 2003 porte sur la création de systèmes de reconnaissance biométrique et généralise ces mesures. Le système mis en place par la Direction de l'administration pénitentiaire implique la reconnaissance de la morphologie de la main du prisonnier, couplée à une carte d'identité magnétique. Dès son arrivée dans la prison, le détenu enregistre au greffe un gabarit de la main, qui est stocké avec le nom, une photographie, un numéro d'écrou dans un serveur central. Les données biométriques ne peuvent être communiquées qu'au personnel de l'administration pénitentiaire ; elles sont détruites au moment de la levée d'écrou. La généralisation est permise par l'arrêté de juin 2003 mais il y a peu de chances qu'elle devienne une réalité. En effet, ces installations sont coûteuses et il est peu probable que le ministère de la justice équipe chaque prison. Le personnel pénitentiaire adopte une position nuancée. L'utilisation des techniques biométriques est considérée comme protectrice dans les grands établissements. Dans les petits établissements, le personnel pénitentiaire connaît bien les détenus ; le recours à des techniques biométriques n'a pas de justification. Les mesures annoncées ont un impact sur l'opinion publique, mais n'empêcheront pas les évasions qui prendront d'autres formes que les évasions de substitution.

Quand la finalité n'est pas sécuritaire, l'objectif de proportionnalité est encore plus important. Un débat animé a été lancé en Europe dans les cantines scolaires. Le collègue Jean Rostand de Nice avait choisi une base de données biométriques reposant sur la reconnaissance automatique des empreintes digitales. La CNIL a relevé que la constitution d'une base de données

d'empreintes digitales était susceptible d'être utilisée à des fins étrangères à la finalité recherchée ; elle a rendu en mars 2000 un avis défavorable, en raison de la disproportion entre le moyen et la finalité recherchée. Le collège de Carqueiranne propose un contrôle d'accès basé non pas sur les empreintes digitales, mais sur la technique biométrique du contour de la main. La CNIL rend un avis favorable : le détournement de finalité est impossible. Au Royaume-Uni, le collège Venerable Bede de Sunderland a décidé en juillet 2003 d'installer un système biométrique de reconnaissance de l'iris pour l'accès des élèves à la cantine. Le choix s'est porté sur l'iris plutôt que sur les empreintes digitales pour des raisons d'efficacité. Les associations de défense des droits de l'homme militent contre cette mesure, considérée comme attentatoire à la vie privée et aux libertés individuelles³.

Techniques biométriques et protection des données personnelles

Les techniques biométriques sont appréciées différemment au regard de la protection des données personnelles :

Les empreintes digitales : ce sont les empreintes digitales qui sont à l'origine des principales critiques des autorités de régulation. Ces dernières considèrent que les empreintes digitales génèrent un risque de traçabilité qui peut être exploité aux dépens des personnes physiques. Une base de données peut être utilisée à d'autres fins que l'objectif poursuivi à la création. Le détournement de finalité est possible. C'est pourquoi les empreintes digitales sont surtout utilisées à des fins d'identification policière.

La reconnaissance palmaire : c'est le procédé le mieux accepté par les autorités de régulation. La reconnaissance de la main s'appuie sur une image en trois dimensions. Elle n'appartient pas aux données biométriques qui laissent des traces et qui peuvent donner lieu à identification. Au Québec, les usagers de l'université de Montréal sont reconnus grâce à la forme de leurs mains.

La reconnaissance faciale : elle donne lieu à de nombreux développements, notamment aux USA, surtout depuis les attentats du 11 septembre 2001. Elle se base sur les caractéristiques principales du visage pour construire une carte du faciès. Il convient d'établir une distinction entre la reconnaissance de visage fixe et la reconnaissance de visage mobile. L'identification d'un sujet fixe est assez fiable. L'identification d'un sujet mobile induit un taux d'erreurs élevé, ce dont les USA ont pris conscience en 2003. Malgré tout, l'usage de cette application est assez répandue dans le monde. Elle n'exige pas le consentement des personnes intéressées, ce qui satisfait les institutions policières et induit des critiques de la part des autorités de régulation. En France, la CNIL n'a instruit aucun dossier de reconnaissance faciale. En Belgique, la police fédérale a validé, en mai 2002, l'installation d'un système de reconnaissance faciale dans ses bureaux. Des aéroports de Suisse, des Pays-Bas et du Royaume-Uni utilisent ce procédé, qui est dénoncé par les organismes de défense des droits de l'homme.

³ cf : Privacy International, <http://www.privacyinternational.org>

L'iris : c'est une technique biométrique efficace. L'iris est unique ; les deux iris de la même paire d'yeux sont différents. Les iris de jumeaux monozygotes ne sont pas identiques. Un iris, sur le plan de la biométrie, est extrêmement complexe. Le taux d'erreur est infinitésimal. Cependant, il convient, pour parvenir à ce résultat, de se procurer des systèmes haut de gamme. D'après une étude du Gartner Group⁴, les critères retenus pour juger de la qualité d'une technique biométrique sont les suivants : non-intrusivité, le niveau de sécurité, le coût, la facilité d'utilisation. C'est la reconnaissance par l'iris qui présente la notation la plus avantageuse. Le seul inconvénient réside dans la cherté de l'application.

La rétine : une lumière infrarouge de forte intensité scanne l'iris. La technique est efficace mais elle porte atteinte aux libertés individuelles. Un rapport officiel a été établi par Marc Chassé. D'après lui, «le balayage de la rétine, ou de l'iris, permet de savoir si une personne est droguée ». Les renseignements médicaux, qui peuvent être ainsi collectés, rentrent dans la catégorie des données personnelles sensibles. C'est pourquoi la reconnaissance par la rétine est très peu utilisée par les décideurs, sauf dans certains milieux carcéraux.

L'ADN : c'est la technique biométrique la plus fiable, mais elle est intrusive, encore plus que la reconnaissance par la rétine. Elle n'est donc utilisée que par les milieux policiers et donne lieu à bien des critiques. Par exemple, la base de données de la police anglaise a été initiée avant que la loi devant avaliser ce stockage n'ait été votée. Les policiers sont invités à prélever un échantillon d'ADN sur toute personne arrêtée, quel que soit le crime ou le délit dont elle est suspectée et avant tout jugement. La commission chargée par le gouvernement de fixer les lignes directrices de la police génétique de la Grande-Bretagne a émis des réserves. Pour la présidente de cette commission, le contrôle de la base de données devrait être confié à une entité indépendante et non à la police. De plus, seuls les individus jugés et reconnus coupables devraient être fichés. Le prélèvement d'ADN porte atteinte à la présomption d'innocence. Quant à la base de données, elle peut être considérée comme contraire à la convention européenne des droits de l'homme.

Les diverses applications biométriques ne sont donc pas sans poser de nombreuses questions aux industriels d'une part, aux autorités de régulation dans le domaine de la protection des données personnelles, d'autre part.

Biométrie et droit du travail : Le contrôle des horaires de travail

Un employeur dispose d'une prérogative de surveillance concernant les horaires auxquels sont assujettis les salariés. Ces derniers se doivent de respecter les horaires collectifs. Le contrat de travail repose sur un lien de subordination. Selon la directive de 1995, l'employeur, en tant que responsable de la surveillance, ne peut agir que si cela est «nécessaire à la réalisation de l'intérêt légitime poursuivi...à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée » (c'est à dire, le salarié). Les entreprises sont tentées d'utiliser la

⁴ 2002

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

biométrie pour gérer les horaires. Conscientes de ce besoin, certaines sociétés de biométrie proposent un volet « gestion du temps de travail ». Depuis une vingtaine d'années, l'obligation de pointer sur les lieux de travail, dans les administrations ou entreprises, a pris en compte l'identification. La présentation d'un badge est anonyme. N'importe quel(le) collègue peut présenter le badge, en lieu et place des personnes concernées. C'est pourquoi le recours à des procédés biométriques a été envisagé. Ainsi, la préfecture de l'Hérault a-t-elle saisi en 2000 la CNIL d'une demande d'avis relatif à la mise en place d'un traitement automatisé d'informations nominatives destiné à permettre l'authentification des agents travaillant pour la préfecture. L'inconvénient résidant dans le défaut de proportionnalité entre la finalité du contrôle des horaires et la création d'une base de données d'empreintes digitales, la CNIL a rendu un avis négatif qui a été suivi par la préfecture de l'Hérault. Pour le même motif, une compagnie aérienne a saisi la CNIL d'une demande de traitement automatisé avec contrôle des empreintes digitales. La CNIL a considéré qu'il y avait un manque de proportionnalité entre la finalité poursuivie et les dangers générés par la constitution d'une base de données d'empreintes digitales. Les personnels pénitentiaires, quant à eux, ont fait connaître leur refus d'étendre l'usage de la biométrie, cantonné jusqu'à maintenant aux déplacements des détenus, à la gestion des horaires de travail.

Au sein de l'entreprise, le débat n'est pas clos. La majorité des employeurs est favorable à l'utilisation des techniques biométriques afin de contrôler les horaires du personnel. Les procédés les plus usités sont le lecteur d'empreintes digitales, l'iris et la reconnaissance palmaire.

Devant la multiplicité des enjeux, le législateur souhaite que des textes soient spécifiquement consacrés à la biométrie. En France, le rapport du député Christian Cabal (juin 2003) va dans ce sens. Les principaux acteurs, les industriels, qui souhaitent utiliser sans contrainte la biométrie, et les défenseurs des libertés individuelles travaillent à l'établissement d'un équilibre qui est actuellement en mouvance.



Les documents de notre site sont sous [Creative Commons License](#)



N.B.