

LA BIOMÉTRIE : QUELS USAGES ?

QUE CE SOIT POUR LA SÉCURISATION D'ENVIRONNEMENTS CRITIQUES OU LA PERSONNALISATION D'ENVIRONNEMENTS PRIVÉS, LA BIOMÉTRIE SE COMMANDE AU DOIGT ET À L'ŒIL.

PAR MICHEL EYNAUD

Getty Image



Si l'image de la biométrie est associée à celle de sécurité, nous allons voir qu'elle doit également être associée à celle de confort. Et nous verrons que l'évolution des technologies touche aussi l'identification.

POUR DES APPLICATIONS JUGÉES CRITIQUES

Du fait des contraintes de mise en œuvre, surtout réglementaires en France, et de coûts, l'usage de la biométrie sera préférentiellement rencontré dans certaines applications critiques et/ou poussées par une volonté politique. Une bonne démarche de sécurité étant avant tout une bonne gestion du risque, l'évaluation de risques élevés incitera à l'emploi de solutions de plus haut niveau de sécurité, dont en contrôle d'accès les technologies biométriques. Ainsi, la biométrie se rencontrera par exemple, dans les sites liés aux activités industrielles et tertiaires sensibles (chimie, armement, R & D, salles informatiques, finances, direction...), aux transports (aéroports, sites logistiques...), à la santé (pharmacie d'hôpitaux...) et pour les applications liées aux circulations internationales de personnes. Pour ces applications critiques, ce sont les technologies biométriques les plus fiables qui sont utilisées, comme la reconnaissance d'empreintes avec un grand nombre de paramètres, la reconnaissance d'iris, des réseaux veineux de la paume de la main ou du doigt, ou les reconnaissances 3D de la morphologie faciale ou de la main.

DES PASSEPORTS VRAIMENT BIOMÉTRIQUES

Les passeports classiques ont été parmi les identifiants les plus falsifiés. A une époque, s'ajoutaient à une certaine facilité de falsification des passeports sans lecture optique (tout est relatif) les difficultés d'authentification par les douaniers de documents parfois d'origine lointaine. Les passeports biométriques sont une réalité aujourd'hui dans plusieurs pays. Déjà nécessaires pour rentrer aux Etats-Unis, le passeport à lecture optique et le passeport électro-



La biométrie ne rime plus

seulement avec la notion de sécurité. Elle peut désormais être associée à celle de confort.

que, limité au stockage de la photo et délivré depuis 2006, sont en train de céder la place en France au passeport biométrique depuis le 1^{er} janvier. Celui-ci stocke dans une puce mémoire sécurisée de type RFID la photo numérisée et 8 empreintes digitales du porteur. Sur le premier semestre, Atos et Sagem vont fournir 5 000 machines à 2 000 mairies et 350 sous-préfectures. Le coût élevé de l'opération devrait être en partie financé par l'augmentation, depuis le 1^{er} janvier, du timbre fiscal nécessaire à la délivrance du passeport. Il sera possible de comparer un sur un les données du passeport avec la biométrie du porteur, et les données seront centralisées dans une base de données, ce qui suscite quelques débats.

De son côté, la Commission européenne préconise une utilisation large de la biométrie pour la surveillance des frontières européennes dans un futur proche. Les données biométriques seraient collectées lors des demandes de visa ou à l'entrée sur le sol européen pour les pays dispensés de visa. Si le but premier est la sécurité, l'autre but est une plus grande rapidité de vérification pour les ressortissants de l'espace Schengen, pour plus de confort.

L'aéroport international d'Oman a été équipé par Evolynx d'un système de contrôle d'accès utilisant la carte d'identité biométrique d'Oman, qui sert également de permis de conduire. Le service de portes électroniques, ainsi qu'il est appelé, est réservé aux citoyens omanais et aux étrangers d'un niveau professionnel élevé présents à Oman pour affaires et détenteurs d'une carte de résident. C'est la reconnaissance d'empreintes digitales qui a été retenue. Une passerelle avec les bases de données de la Police royale omanaise a été mise en place.

IRIS ET PARTICULES

Le Cern est l'Organisation européenne pour la recherche nucléaire, qui effectue des recherches avancées sur les particules élémentaires au moyen d'accélérateurs de particules souterrains à la

frontière franco-suisse près de Genève. Les recherches en cours sont toujours de haut niveau et faites par de très grands scientifiques, principalement sur les particules ou les hautes énergies, et également sur des projets annexes, comme le projet Enquire de Tim Berners-Lee et Robert Cailliau en 1989, qui a abouti aux fondements du World Wide Web, système de navigation hypertexte utilisant le réseau Internet comme couche de transport. Près de 2 600 employés à temps complet et 8 000 scientifiques et ingénieurs de 80 nationalités ont accès au site. Le 21 octobre dernier, était inauguré le nouveau Grand Collisionneur de Hadrons (LHC), l'instrument scientifique le plus grand et le plus complexe au monde, dont l'accès est sécurisé par un système de reconnaissance d'iris d'Evolynx mis en place par Cegelec Secure, et utilisant conjointement des badges à lecture-écriture. Une quarantaine de sas dans les différents puits d'accès au tunnel sont équipés de lecteurs d'iris, qui sont utilisés en ce moment pour 28 000 passages par semaine. Outre les aspects sécuritaires, ce système a été retenu pour les possibilités d'accès mains libres ou gantées. La lecture de l'iris fonctionne même à travers des lunettes. Les sas sont également équipés de détecteurs infrarouges de mouvements et de capteurs de poids de façon à assurer l'unicité de passage. A noter que des puces Mifare vont être intégrées aux dosimètres portés par les personnes potentiellement en contact avec des radiations, leur permettant de



servir de badge d'accès renfermant les données biométriques. Et, à l'avenir, la même carte servira pour l'accès à la bibliothèque et au login informatique.

L'ACCÈS SANS CLÉ NI BADGE

Les projets autorisés par la Cnil sont ceux qui protègent l'utilisateur contre une utilisation frauduleuse de ses données biométriques. Peu de projets basés sur des systèmes de reconnaissance d'empreinte 1:n avec stockage interne sans badge sont autorisés par la Cnil. Pour la reconnaissance d'empreintes digitales, les systèmes mis en œuvre doivent, de préférence, stocker l'empreinte de l'utilisateur sur son badge, et non dans le lecteur ou sur le réseau, pour effectuer une identification 1:1. Ainsi, une empreinte copiée (sur un verre, une poignée de porte, etc.) et reproduite ne pourra pas être comparée avec une référence dans le système. Pour les techniques ne permettant pas, au moins avec les connaissances actuelles, une reproduction de la biométrie d'un individu et qualifiées de « sans trace » par la Cnil, le stockage des données peut être autorisé. Il s'agit, par exemple, des reconnaissances de la morphologie 3D de la main ou du visage, de l'iris, ou des réseaux veineux de la main ou d'un doigt. Si l'empreinte ne peut pas être reproduite, les données stockées dans le système, au niveau du lecteur ou en central, peuvent être sécurisées par un algorithme. Certaines activités bénéficient pleinement de l'absence de recours à un badge. Il s'agit, dans le monde du travail, des activités manuelles avec des gants – chantiers ou blocs opératoires, par exemple – ou de transport avec des bras chargés, qui pourront utiliser la reconnaissance d'iris ou de la voix. Dans certaines conditions de grande finesse des gants, la reconnaissance des réseaux veineux de la main ou du doigt pourra fonctionner à travers. Toutes les activités sportives bénéficient de l'absence de badge. Pour les piscines et autres milieux humides, ainsi que lors d'activités salissantes, sportives ou professionnelles, la reconnaissance de réseau veineux fonctionnera parfaitement sur mains humides ou salies. En environnement stérile, on privilégiera la reconnaissance d'iris ou du réseau veineux de la main, possibles sans contact. La restauration collective, en entreprise ou scolaire, et le milieu carcéral (voir interview, p. 25) utilisent, de préférence, la reconnaissance de la morphologie de la main, qui ne nécessite pas de badge. Enfin, les applications sans badge seront parfois réclamées par les dirigeants d'une entreprise pour plus de confort ou, tout simplement, pour impressionner les visiteurs.

ACCÈS LOGIQUE

L'autre grand domaine du contrôle d'accès concerne l'accès logique aux réseaux, stations de travail et, de plus en plus souvent, aux PC portables, grâce à la disponibilité de modules miniaturisés. Les technologies employées sont les mêmes qu'en contrôle d'accès électronique, en utilisant de préférence des lecteurs de petite taille posés sur un bureau ou bien intégrés à un PC portable. Si la reconnaissance d'empreintes est majoritairement employée, des lecteurs de réseau veineux de la paume de la main sont disponibles pour port USB, tel que le ZX-PS Palm Secure de Zalix, qui apporte à la fois confort et sécurité par la non-reproductibilité du gabarit veineux. La reconnaissance d'empreintes digitales sera mise en œuvre avec ou sans badge associé, selon l'aspect professionnel ou privé de l'utilisation du PC. Les capteurs peuvent également être intégrés à une souris, ou bien directement à une clé mémoire USB, en ne protégeant que les données de celle-ci.

PATTE BLANCHE POUR GANT DE VELOURS

Par ailleurs, de nombreux produits sont devenus abordables et ont permis l'élaboration de solutions rencontrées au quotidien, surtout pour des applications de confort. En effet, l'identification certaine d'un individu permet une adaptation des caractéristiques de son environnement à ses préférences enregistrées au préalable. Ces adaptations personnalisées sont intéressantes, dès lors que l'individu partage son environnement. Dans la vie privée, ce sont le domicile et la voiture qui vont pouvoir bénéficier de ces personnalisations, dès lors que des relais peuvent être mis en œuvre. Au domicile, ce sera une installation domotique qui gèrera les paramètres personnalisés, comme la température et l'éclairage, ou encore la diffusion d'une ambiance musicale et le volume sonore. Dans un véhicule de haut de gamme, outre l'accès au véhicule ou encore au démarrage, certains réglages d'ergonomie pourront être réalisés automatiquement, comme les positionnements du siège conducteur et du volant, ainsi que la consigne de température. Pour ces applications de confort, c'est la reconnaissance d'empreintes qui est encore la plus souvent rencontrée, principalement pour des raisons de coût et d'encombrement du lecteur. Si l'emploi de solutions de type professionnel est toujours possible, avec l'utilisation de badges associés à la lecture d'empreintes, le confort relève principalement du domaine privé, et l'impasse sera souvent faite sur la sécurité apportée par le stockage d'empreintes sur le badge. La présence de plus en plus fréquente de



Terminal biométrique Biovein de CDVI.

L'œil de la Cnil

En utilisation professionnelle, dans le cadre d'une entreprise utilisant la biométrie pour les validations d'accès de ses employés, tous les projets doivent faire l'objet d'un dossier de demande d'autorisation déposé à la Cnil. Pour être accepté, un projet devra être assez critique pour justifier l'utilisation de technologies biométriques, en regard des toujours possibles atteintes à la vie privée des utilisateurs. La procédure est simplifiée pour les projets mettant en œuvre les technologies de reconnaissance d'empreintes digitales 1:1 avec badge et de reconnaissance de la morphologie de la main. Ils reçoivent une autorisation rapidement sur simple engagement de conformité à l'autorisation unique AU-007.

fonctions domotiques sur les centrales de détection d'intrusion, qui gèrent déjà de plus en plus le contrôle d'accès, va favoriser l'apparition de fonctionnalités de personnalisation du confort en fonction des personnes présentes et identifiées par badgeage et/ou reconnaissance biométrique. On peut imaginer un accès pour les fournisseurs de service avec badge seul dans un créneau horaire précis et sans personnalisation du confort, et un accès que l'on qualifiera d'enrichi sur reconnaissance personnalisée.

LE FUTUR AU PRÉSENT

Nous avons vu, dans un récent article (APS 171 – Biométrie : des solutions de plus en plus simples), que plusieurs nouvelles technologies émergent en biométrie, ce qui va permettre le développement de nouveaux usages. D'une part, certaines technologies biométriques existantes évoluent, par exemple avec une montée en puissance des puces disponibles pour le traitement des signaux biométriques, qui nécessitent parfois de lourds calculs, l'évolution se faisant également vers une plus grande miniaturisation des capteurs. Ainsi, les capteurs optiques de certains téléphones peuvent analyser l'iris du porteur et lui donner accès non seulement aux télécommunications, mais aussi aux nouvelles applications de paiement en Near Field Communication (NFC).

D'autre part, certaines nouvelles technologies font leur apparition, comme les reconnaissances des réseaux veineux, promises à un bel avenir, ou bien arrivent à maturité, comme la reconnaissance vocale. La Cnil a autorisé l'utilisation d'un système de reconnaissance vocale chez Michelin, dans le cadre de la réinitialisation automatique des mots de passe permettant l'accès au système d'information, via un automate appelé par téléphone. Chez CDVI, le système Orphée a été développé en partenariat avec l'université Pierre et Marie Curie. La reconnaissance vocale est indépendante du texte et de la langue utilisée : le référencement et la vérification du locuteur peuvent être réalisés dans des langues différentes, quel que soit l'état physique du locuteur. De façon générale, les technologies ne nécessitant pas de badge semblent promises à un bel avenir. Dans ces domaines comme dans bien d'autres, il est question de compromis. La biométrie peut représenter un des meilleurs compromis en termes de coût et de simplicité de déploiement et d'usage, tant pour les applications classiques de sécurité que pour celles de confort, en développement rapide. Plus de confort peut également contribuer à un meilleur niveau sécuritaire.

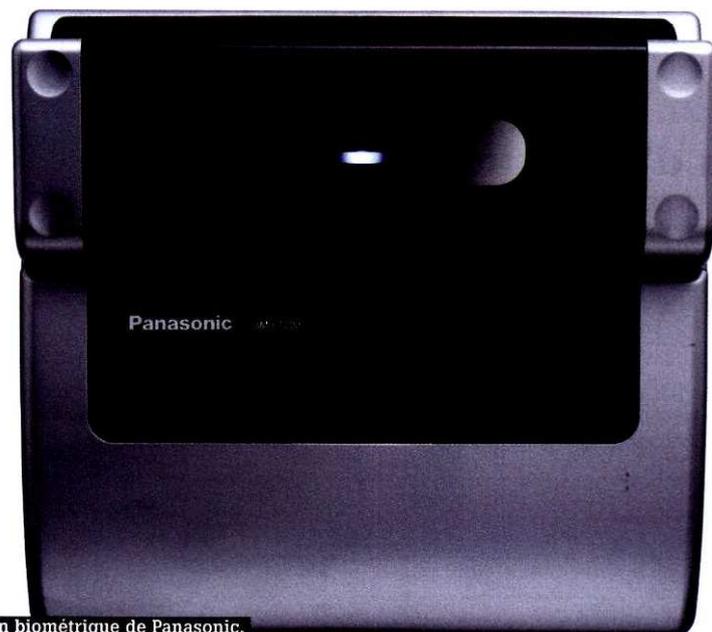


Zalix VPIIS pour reconnaissance du réseau veineux du dos de la main.

Autonome ou centralisé

De nombreux lecteurs biométriques peuvent fonctionner aussi bien en mode autonome qu'en étant intégrés dans un système en réseau. Si le mode autonome peut être considéré comme suffisant dans quelques applications en intérieur, en extérieur, les fondamentaux du contrôle d'accès s'appliquent toujours : il faut privilégier des systèmes où l'électronique de stockage, de décision et de commande des relais d'ouverture est placée dans un boîtier déporté à l'intérieur du bâtiment protégé.

Lecteur d'empreintes digitales DGID LMED de CDVI.



Solution biométrique de Panasonic.

INTERVIEW

Gunnebo : une intégration totale

Dans le secteur tertiaire/industrie, nous avons fait le choix d'une solution totalement intégrée », nous indique Dominique Auvray, directeur marketing du Centre de compétence électronique de Gunnebo, « n'utilisant que des composants éprouvés et de haute sécurité : badges, lecteurs, UTL (unité de traitement local). Pour la reconnaissance d'empreintes 1:1, nous travaillons directement avec des constructeurs de lecteurs biométriques qui maîtrisent la technologie des capteurs et des algorithmes associés. L'intégration est totale, avec un enrôlement complètement natif dans notre superviseur : lors de la création d'une fiche, le responsable de sécurité est guidé pour l'acquisition d'empreinte. A l'export, nous intégrons des applications avec reconnaissance 1:N sans badge. Souvent, les utilisateurs d'un niveau VIP ne veulent plus avoir de badge. Là aussi, notre intégration avec les solutions de type Sagem est totale. Nous travaillons beaucoup sur la sécurisation du transport des données biométriques, à l'intérieur d'un site ou de site à site.

Dans le monde bancaire, la biométrie est encore majoritairement en expérimentation, le point de l'enrôlement restant à faciliter. Toutes les agences sont indépendantes, avec un turnover certain et des gens qui se déplacent d'un site à l'autre ; les intervenants sont multiples et peu centralisés : il en est ainsi des accès pour les transporteurs de fonds, les techniciens de maintenance des guichets automatiques bancaires et le personnel d'entretien, d'où des difficultés de gestion spécifiques à ce marché. Le coût est également un paramètre important. Nous expérimentons plusieurs solutions sur quelques dizaines d'agences bancaires en France. Par ailleurs, nous surveillons les technologies émergentes et prometteuses, comme la reconnaissance veineuse au travers de protocoles d'expérimentation avec des constructeurs. »

INTERVIEW

Zalix : de très nombreuses applications

« La base de la biométrie, c'est l'identification de façon certaine d'un individu, la garantie de l'identité de cette personne pour lui autoriser l'accès à des droits. Si l'application première est le contrôle d'accès à des locaux, il y a beaucoup d'autres applications qui en bénéficient, comme la gestion du temps de présence et de travail des employés, la gestion de présence des élèves dans un établissement scolaire, l'utilisation de la cantine scolaire ou du restaurant d'entreprise, l'accès des clients à une chambre d'hôtel, etc. Dans l'industrie, une opération peut être authentifiée à l'intérieur d'un process de R&D, et le contrôle d'accès des employés d'entreprises de sous-traitance à des locaux de clients peut être assuré en étant certain qu'il s'agit bien de la bonne personne connue et habilitée et non d'un remplaçant inconnu.

Un autre domaine d'application consiste à permettre de s'affranchir des contraintes de badge et de clés, comme pour l'accès du seul personnel hospitalier autorisé à un bloc opératoire ou à la pharmacie centrale. Dans les maisons d'arrêt, l'identité des détenus peut être vérifiée lors des déplacements au parloir ou au tribunal à l'aller comme au retour, pour être certain, par exemple, qu'un échange avec un frère jumeau n'a pas été réalisé. Nos solutions équipent la majorité des maisons d'arrêt de France dans ce but. Les détenus ont les mêmes droits que les citoyens libres, et la technologie employée est celle de la reconnaissance de la morphologie de la main, non reproductible et qui peut être stockée dans le lecteur (cette technologie bénéficie d'une autorisation unique de la CNIL).

Dans le secteur des loisirs, certains casinos et cercles de jeux utilisent la reconnaissance d'empreinte stockée sur badge pour identifier les joueurs réguliers et contrôler les joueurs interdits. Vulcania utilise la lecture anonyme d'empreintes digitales dans le cadre d'un programme de fidélité : une personne étant déjà venue sera reconnue et se verra proposer des options personnalisées.

Dans un véhicule, outre la sécurité, on recherchera plus de confort : l'ouverture de la portière peut être commandée par une télécommande munie d'un lecteur d'empreinte, et une identification permettra une personnalisation du confort (réglages du siège et du volant, de la climatisation et de l'audio).

Nous développons également notre activité en contrôle d'accès logique, aux réseaux informatiques et stations de travail. Dans le futur, les technologies de reconnaissance de la voix devraient arriver à maturité. Cette technologie nous semble être très porteuse d'avenir. »



Le ZX-6000 pour reconnaissance du réseau veineux de la paume de la main chez Zalix.



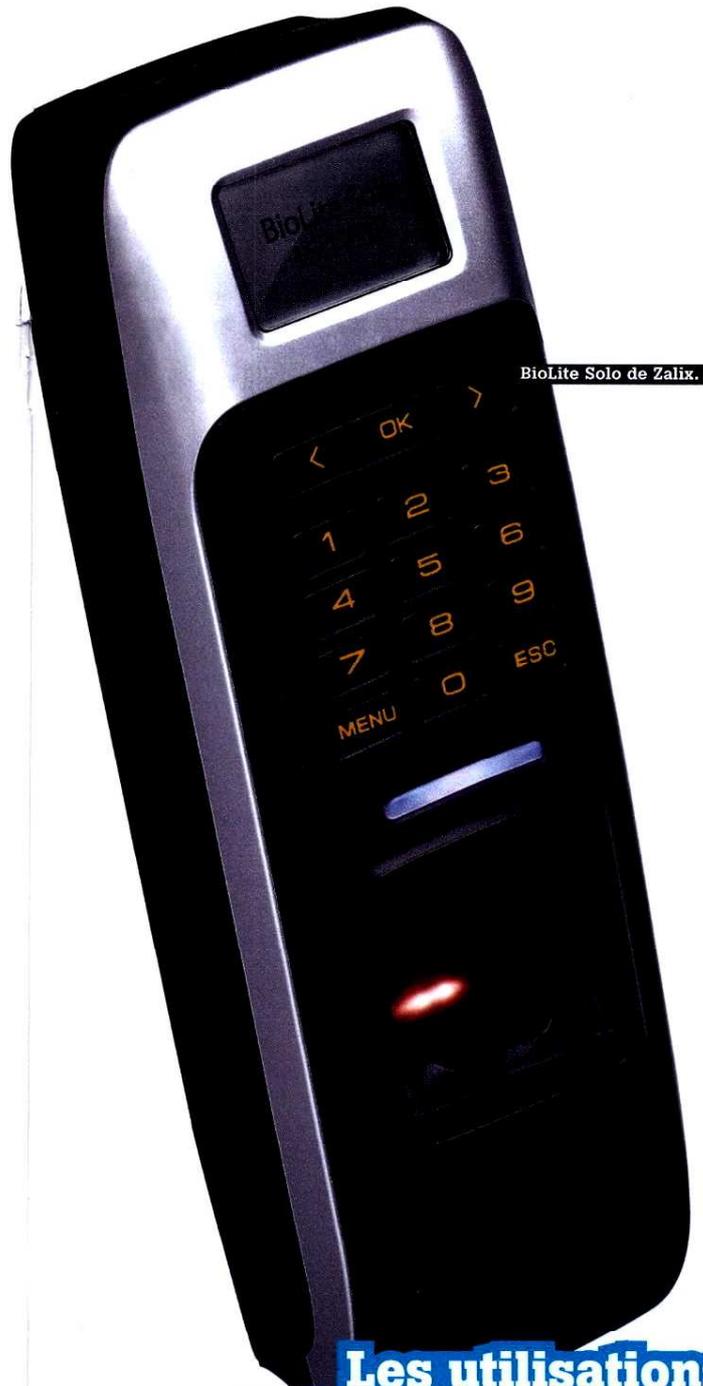
Scanner USB d'empreintes digitales de CDVI.

Les réseaux veineux en veine

Les reconnaissances des réseaux veineux sont les technologies les plus récentes, et sont promises à un brillant avenir. Utilisées depuis quelques années dans le monde bancaire au Japon (essentiellement les distributeurs de billets), ces technologies qui arrivent en sécurité électronique en Europe ont tout pour elles. Elles apportent fiabilité, rapidité, sécurité par la non-reproductibilité, et parfois hygiène par l'absence possible de contact. Les réseaux veineux ne varient pas au cours de la vie d'un individu. Pour des questions de reproductibilité du positionnement, c'est la reconnaissance du réseau veineux du dos de la main qui a été retenue dans le VPIIS de Zalix qui intègre une poignée. Le ZX Palm et le ZX-6000 effectuent une reconnaissance du réseau veineux de la paume de la main. Chez Eden, le lecteur autonome Biovein utilise la reconnaissance du réseau veineux d'un doigt. Tous ces systèmes peuvent fonctionner en autonome aussi bien qu'en réseau centralisé. Les technologies utilisées et brevetées sont, pour la reconnaissance du réseau de la paume, la technologie Fuji, mesurant la réflexion de rayonnements infrarouges émis au niveau du lecteur, et, pour la reconnaissance du réseau du doigt, la technologie Hitachi détectant la transmission de rayonnements infrarouges.

Des fichiers biométriques nationaux et internationaux

En 1987, a été créé le Fichier automatisé des empreintes digitales (FAED), dans lequel sont consignées pendant 25 ans les empreintes digitales des personnes impliquées dans les procédures pénales, et qui stockerait aujourd'hui les empreintes d'environ 2 500 000 personnes. Ce fichier n'est accessible qu'à 300 fonctionnaires habilités. Depuis 1998, ce sont les empreintes génétiques des auteurs d'infractions sexuelles qui sont stockées pendant 40 ans dans le Fichier national automatisé des empreintes génétiques (FNAEG), qui a été, depuis, étendu aux auteurs d'autres crimes et délits, représentant les trois quarts des affaires traitées dans les tribunaux, selon le Syndicat de la magistrature, et qui contiendrait aujourd'hui les empreintes génétiques de plus de 1 % de la population française. Au niveau européen, les pays de la Communauté mettent en commun, au sein du système Eurodac, les fichiers d'empreintes des demandeurs d'asile et des personnes en situation irrégulière, de façon à prévenir les demandes d'asile multiples. Les données sont conservées 10 ans (Sources : Wikipedia et Cnil).



BioLite Solo de Zalix.

Les utilisations privées

La reconnaissance d'empreintes digitales utilisée pour l'accès à un PC est soumise à autorisation de la Cnil s'il s'agit d'un PC d'entreprise mais, s'il s'agit d'un PC personnel dont le particulier propriétaire désire protéger les données, l'utilisation est complètement libre. Une technologie sans badge avec stockage des données dans le PC pourra être employée. Il n'en reste pas moins que le danger de fraude existe autant. Même problématique pour l'accès à un domicile par lecture d'empreinte : chacun est libre de prendre les risques qu'il veut dans sa vie privée. Les techniques de reconnaissance veineuse sans badge associé devraient se développer en utilisation privée avec leurs avantages de sécurité et de confort.