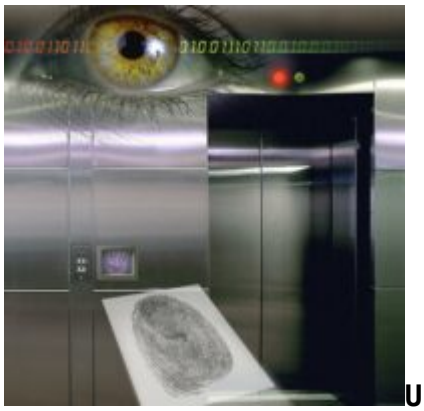
Usurpation d’identité, identification et authentification numérique

 **Usurpations d’identité, identification et authentification numérique : quels enjeux et quelles solutions ?**

Alain Bensoussan(Lexing Alain Bensoussan Avocats) et **Philippe Morel** (Woobe) interviendront lors du **petit-déjeuner débat** du vendredi **7 février 2020.**

La confidentialité et la sécurité des données sont au centre des débats, cybersécurité oblige.

Définie comme « *le traitement automatique d’images numériques qui contiennent le visage de personnes à des fins d’identification, d’authentification/de vérification ou de catégorisation de ces personnes* » (définition du CEPD) , la reconnaissance faciale cristallise toutes les attentions.

Identification et authentification numérique : Quelles solutions ?

A l’heure où nombreuses sont les voix qui s’élèvent pour appeler à restreindre l’utilisation croissante de la reconnaissance faciale par les acteurs économiques et les autorités, et où d’autres solutions voient le jour (ex. : identité universelle et irrévocable supranationale et opposable aux tiers), **le cabinet Lexing Alain Bensoussan Avocats vous convie à un petit-déjeuner débat autour des enjeux juridiques et éthiques dans ce domaine**.

Seront notamment évoqués à cette occasion par Alain Bensoussan :

- Les contours de l’encadrement juridique en gestation en la matière
- Les solutions alternatives à la reconnaissance faciale et leur conformité juridique

Par ailleurs, **Philippe Morel**, ancien juge consulaire, président-fondateur de la plateforme Woobe, présentera à cette occasion une solution garantissant la confidentialité et la valeur juridique des échanges numériques en identifiant de manière irrévocable les auteurs des contenus, les expéditeurs, les destinataires et tous les tiers autorisés à chaque étape critique, grâce à la vérification dynamique des empreintes digitales, dans lequel le consentement de l’utilisateur est intégré dans le processus.

Le petit-déjeuner débat a lieu **le 7 février 2020** de 9h30 à 11h30 (accueil à partir de 9h00) dans nos locaux, 58 Gouvion-Saint-Cyr, 75017 Paris.

Événement gratuit. Inscription : **lien**

La Cnil et la reconnaissance faciale aux abords des lycées

Alain Bensoussan évoque pour Digital Mag la reconnaissance faciale aux abords des lycées et les précisions apportées par la Cnil.

Saisie d'une expérimentation prévoyant le recours à la reconnaissance faciale à l'entrée de deux lycées marseillais et niçois, la Cnil a considéré que « *ce dispositif concernant des élèves, pour la plupart mineurs, dans le seul but de fluidifier et de sécuriser les accès n'apparaissait ni nécessaire, ni proportionné pour atteindre ces finalités* » (Séance plénière du 17 octobre 2019).

Reconnaissance faciale aux abords des lycées : les données sensibles d'un public… sensible

S'agissant de mineurs de plus de 15 ans, même si leur consentement était acquis, la question se pose d'un choix réel et non contraint. Par ailleurs, la sécurisation des données biométriques est toujours problématique et ce proportionnellement au risque important d'atteinte aux libertés individuelles des personnes concernées.

> Après un examen attentif du projet, la Cnil a considéré que le dispositif projeté est contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD (Règlement général sur la protection des données).
>
> En effet, les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge.

Les technologies de reconnaissance faciale présentent beaucoup d'intérêt en matière de sûreté et de sécurité, mais elles sont aussi porteuses d'un risque important d'atteinte aux libertés individuelles.

Ces technologies soulèvent encore de nombreuses questions non résolues. C'est pourquoi la Cnil a appelé à un débat démocratique sur ce sujet, ainsi que plus largement sur les nouveaux usages de la vidéo.

Isabelle Pottier
Avocat, Lexing Alain Bensoussan Avocats
Directeur du département Etudes et publications

Alain Bensoussan, « Reconnaissance faciale aux abords des lycées, les précisions de la Cnil », DigitalMag n° 258 p.42-43 décembre 2019.

Usurpation d'identité, identification et authentification numérique

Usurpations d'identité, identification et authentification numérique : quels enjeux et quelles solutions ?

Alain Bensoussan(Lexing Alain Bensoussan Avocats) et **Philippe Morel** (Woobe) interviendront lors du **petit-déjeuner débat** du vendredi **7 février 2020.**

Aujourd'hui, cybersécurité oblige, la confidentialité et la sécurité des données sont au centre des débats.

Dans ce domaine, la reconnaissance faciale, qui peut être définie comme « *le traitement automatique d'images numériques qui contiennent le visage de personnes à des fins d'identification, d'authentification/de vérification ou de catégorisation de ces personnes* » (définition du CEPD) , cristallise toutes les attentions.

Identification et authentification numérique : Quelles solutions ?

Cette technologie, qui n'en était qu'à ses débuts il y a quelques années à peine, a fait depuis l'objet de progrès spectaculaires.

De toute évidence, les perspectives qu'elle ouvre sont vertigineuses, et plus seulement dans le domaine de la sécurité publique, première terre d'élection de la reconnaissance faciale permettant de reconnaître un visage dans une foule.

Pour autant, la reconnaissance faciale qui se fait par « matching » d'un jpeg dans une base de données, n'est pas un outil destiné à créer une identité, au sens juridique du terme, mais une reconnaissance d'un individu sur des critères

physiques et esthétiques.

En outre, les critères faciaux ne sont pas définitifs, uniques et permanents, de sorte qu'ils se situent en dehors du champ d'application des caractéristiques susceptibles d'être reçues en justice comme moyen de preuve.

De surcroît, cette technologie reste fragile.

Quels sont les obstacles juridiques ?

Enfin et surtout, la reconnaissance faciale comme moyen d'identification légal se heurte en l'état actuel à deux obstacles dirimants :

- le recours à un fichier central des données, d'une part ;
- la disproportionnalité des traitements, d'autre part.

A l'heure où nombreuses sont les voix qui s'élèvent pour appeler à restreindre l'utilisation croissante de la reconnaissance faciale par les acteurs économiques et les autorités, et où d'autres solutions voient le jour (ex. : identité universelle et irrévocable supranationale et opposable aux tiers), **le cabinet Lexing Alain Bensoussan Avocats vous convie à un petit-déjeuner débat autour des enjeux juridiques et éthiques dans ce domaine**.

Seront notamment évoqués à cette occasion par Alain Bensoussan :

- Les contours de l'encadrement juridique en gestation en la matière
- Les solutions alternatives à la reconnaissance faciale et leur conformité juridique

Par ailleurs, **Philippe Morel**, ancien juge consulaire, président-fondateur de la plateforme Woobe, présentera à cette occasion une solution garantissant la confidentialité et la valeur juridique des échanges numériques en identifiant de manière irrévocable les auteurs des contenus, les expéditeurs, les destinataires et tous les tiers autorisés à chaque étape critique, grâce à la vérification dynamique des empreintes digitales, dans lequel le consentement de l'utilisateur est intégré dans le processus.

Le petit-déjeuner débat a lieu **le 7 février 2020** de 9h30 à 11h30 (accueil à partir de 9h00) dans nos locaux, 58 Gouvion-Saint-Cyr, 75017 Paris.

Biométrie : quelques notions de base sur la technologie

Depuis plusieurs années, la biométrie se fait de plus en plus présente dans les objets et outils de notre quotidien.

Elle s'insère dans les passeports que nous emmenons avec nous pour voyager, dans les systèmes d'authentification qui nous permettent d'accéder aux fonctionnalités de notre téléphone portable, de réaliser un paiement à distance ou encore d'accéder à des locaux professionnels sécurisés.

Utilisée aussi bien par des entreprises du secteur privé que dans l'exercice de la puissance publique, la Commission nationale de l'informatique et des libertés (Cnil) garde un oeil toujours très attentif sur les garanties apportées pour les droits et libertés des individus (1). Pour bien comprendre cette technologie et ce qui la rend sensible, il est utile de revenir sur quelques notions de base de la biométrie.

Définitions de la biométrie

Sur son site internet (2), la Cnil propose la définition suivante :

> « La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.) ».

Le règlement général sur la protection des données propose quant à lui une définition juridique des données biométriques, entendues comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques » (3).

Il en ressort plusieurs éléments essentiels attachés à la biométrie, à savoir :

- le recours nécessaire à la technique pour obtenir des données biométriques ;
- l'analyse des caractéristiques physiques, biologiques et physiologiques ou comportementales d'un individu ;
- l'objectif de reconnaissance, d'identification d'un individu, qui permet de qualifier de « donnée à caractère personnel » les données biométriques ;
- le caractère d'unicité et de permanence pouvant être attaché à une donnée biométrique.

Techniques biométriques

Les techniques biométriques peuvent utiliser différentes caractéristiques attachées aux individus, telles que notamment :

- la vérification des empreintes digitales ;
- l'analyse du réseau veineux ;

- l’analyse de la forme de la main ;
- la reconnaissance faciale ;
- l’analyse de l’iris ;
- l’analyse de la rétine ;
- la reconnaissance vocale ;
- la détection de l’odeur corporelle ;
- la reconnaissance de la frappe au clavier ;
- l’analyse de la démarche d’un individu ;
- la vérification de sa signature manuscrite.

Chacune de ces techniques se voit rattacher un caractère d’unicité et de permanence plus ou moins fort. Par exemple :

- sur l’unicité: il est moins compliqué de trouver deux individus ayant la même manière de frapper au clavier de leur ordinateur que deux individus ayant les mêmes empreintes digitales ;
- sur la permanence: la démarche d’un individu est amenée à évoluer dans le temps; l’iris ou la rétine beaucoup moins.

L’association de plusieurs techniques biométriques en vue d’améliorer les résultats ou la précision du dispositif est également possible, par exemple la mise en place d’un dispositif de reconnaissance des empreintes digitales et du réseau veineux d’un individu. On appelle cela la biométrie multimodale.

Régime applicable à ce jour

En dehors des traitements mis en œuvre pour le compte de l’Etat, qui font l’objet d’un avis de la Cnil, la loi Informatique et libertés soumet le recours à la biométrie à une autorisation de la Commission.

Afin de simplifier les démarches administratives des responsables de traitement, la Cnil a adopté plusieurs autorisations uniques en matière de biométrie, parmi lesquelles :

- l’autorisation unique AU-052 relative aux dispositifs biométriques permettant aux personnes de garder la maîtrise de leur gabarit biométrique ;
- l’autorisation unique AU-053 relative aux dispositifs biométriques ne garantissant pas cette maîtrise.

Le gabarit représente l’ensemble des mesures effectuées et enregistrées par un lecteur biométrique lors du premier enregistrement d’un utilisateur afin de permettre l’authentification de ce dernier. A partir des points caractéristiques présents sur une empreinte digitale par exemple, un algorithme permettra de calculer un identifiant (une suite alphanumérique) qui constituera un gabarit d’empreinte digitale (4). Pour la Cnil, les dispositifs garantissant la maîtrise des personnes sur leur gabarit doivent être privilégiés (support de stockage confié à la personne, par exemple).

Les autorisations uniques décrivent chacune des traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Un organisme souhaitant mettre en place un dispositif biométrique qui serait couvert en tous points par l’une des autorisations uniques pourra adresser à la Cnil un engagement de conformité à cette autorisation unique. En revanche, si le

dispositif envisagé n’est pas couvert par une autorisation unique, le responsable du traitement doit adresser à la Cnil une demande d’autorisation spécifique décrivant le dispositif en cause.

Et demain ?

L’application du règlement général sur la protection des données à compter du 25 mai 2018 viendra sans doute renforcer la protection des données biométriques, à travers notamment un principe d’interdiction de traitement assorti d’exceptions ou encore de la nécessité, dans certains cas, de réaliser une analyse d’impact.

Une large part est également laissée aux Etats membres pour le maintien ou l’introduction de conditions supplémentaires au traitement de données biométriques. Il est fort probable que la France se saisisse de cette opportunité (5).

Alain Bensoussan Avocats
Lexing Droit Informatique et libertés

(1) En 2015, la Cnil a délivré 359 autorisations pour des traitements ayant recours à la biométrie. Rapport d’activité 2015 p. 5.
(2) Site de la Cnil, Définition de la biométrie
(3) Règlement (UE) 2016/679 du 27-4-2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE du 24-10-1995 (règlement général sur la protection des données), art. 4 § 10
(4) Communication de la Cnil relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données
(5) Lire le Post du 2-8-2016

La biométrie prête sa voix pour sécuriser les transactions

 Les techniques de biométrie sont de plus en plus utilisées dans le monde comme moyens de sécurisation de transactions.

La biométrie s’intègre parfois dans les cartes bancaires (empreinte digitale), dans les distributeurs de billets (reconnaissance faciale) ou encore peut être utilisée en lien avec un service de paiement mobile ou par internet, comme la Cnil vient pour la première fois de l’autoriser en France.

En effet, la loi Informatique et libertés soumet à autorisation de la Cnil les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes (1).

Phase expérimentale

Au cours des dernières années, la Cnil a été saisie de plusieurs autorisations portant sur des systèmes d'authentification des auteurs de transactions bancaires au moyen de la biométrie, notamment vocale.

Jusqu'en février 2016, les autorisations délivrées par la Cnil ne portaient toutefois que sur des traitements mis en œuvre à titre expérimental. La durée de ces expérimentations variait entre 3 et 15 mois et ces dernières pouvaient concerner jusqu'à plusieurs milliers d'individus, salariés et/ou clients de la société responsable du traitement.

D'une manière générale, la phase d'expérimentation permet au responsable de traitement d'évaluer :

- la faisabilité du traitement ;
- la qualité de la technique de biométrie vocale utilisée (ex : mesure des faux positifs et faux négatifs) ;
- la facilité d'utilisation du service envisagé (ex : ergonomie du service, temps moyen d'authentification).

Phase de généralisation

Les résultats des expérimentations menées par une banque se sont visiblement révélés positifs puisque la Cnil vient de l'autoriser à généraliser un système d'authentification des porteurs de cartes bancaires par reconnaissance vocale (2).

Une phase d'expérimentation d'une durée totale de 2 ans a en effet permis à cette banque de confirmer l'appétence du public pour ce type de service (fluidité des parcours, sentiment de sécurité), en relevant un taux de satisfaction de 86%.

Une authentification forte

La Commission se montre ainsi favorable à l'utilisation de la biométrie dans le cadre de la sécurisation du paiement à distance. Elle observe à ce titre que la mise en place d'une authentification forte des clients souhaitant régler des transactions en ligne, reposant sur l'utilisation de plusieurs éléments d'authentification, répond à un phénomène de fraude aux paiements à distance en constante augmentation.

En l'espèce, la méthode d'authentification choisie s'appuie sur deux éléments d'authentification : la réception d'un appel sur un téléphone préalablement enrôlé (« ce que je possède ») et la reconnaissance de la voix (« ce que je suis ») (3). Ainsi, le dispositif biométrique n'a pas vocation à fournir un moyen d'authentification autonome. Il vient renforcer un dispositif existant qui s'appuie sur la possession d'un objet, à savoir le téléphone portable de la personne concernée.

Une méthode d'authentification proposée et non imposée

Conformément à l'article 7 de la loi Informatique et libertés (4), le traitement de reconnaissance vocale autorisé par la Cnil s'appuie sur le consentement spécifique, libre et éclairé des personnes concernées.

La méthode d'authentification est ainsi proposée aux clients de la banque en tant qu'alternative à l'authentification par saisie d'un code à usage unique, le client pouvant à tout moment revenir sur son choix.

Technique biométrique utilisée

La technique de reconnaissance vocale utilisée se base sur la modélisation physique des caractéristiques du conduit vocal de la personne concernée. Un modèle de voix non réversible est alors constitué.

En effet, le modèle ne constitue pas un enregistrement de la voix de la personne concernée. Il reproduit une distribution de probabilités de plusieurs caractéristiques de la voix du client. Les caractéristiques biométriques du client ne pourront donc pas être reconstituées à partir du modèle.

Etude d'impact

Dans les différentes autorisations expérimentales délivrées par la Cnil, la Commission a exigé de chaque responsable de traitement qu'il communique un bilan des modalités de fonctionnement et d'utilisation du dispositif au terme de la phase d'expérimentation.

Notamment, une présentation des enjeux spécifiques relatifs à la protection des données doit être envoyée à la Cnil, incluant les risques identifiés et les mesures adoptées pour les limiter, ainsi qu'une synthèse relative au respect des dispositions de la loi Informatique et libertés.

La banque dont le traitement vient d'être autorisé a ainsi réalisé une étude d'impact à l'issue de ses expérimentations. La Cnil a alors pu relever que « les mesures techniques adoptées [avaient] permis de réduire à un niveau de vraisemblance et de gravité faible les impacts résultant notamment des risques de fuites ou de pertes des données, d'indisponibilité du dispositif ou d'usurpation d'identité ».

Cette démarche apparaît en accord avec l'approche par les risques proposée au niveau européen dans la proposition de règlement général sur la protection des données. Elle permet notamment d'anticiper l'obligation pour les responsables de traitement de réaliser des analyses d'impact relatives à la protection des données, en particulier en cas de traitement à grande échelle de données biométriques.

Pour conclure, les sociétés souhaitant mettre en place des systèmes d'authentification d'auteurs de transactions bancaires au moyen de la biométrie sont invitées à réaliser des analyses de l'impact de leur traitement sur la protection des données et à déposer auprès de la Cnil un dossier de demande d'autorisation.

Alain Bensoussan Avocats
Lexing, Droit Informatique et libertés

(1) Loi 78-17 du 6-1-1978, art. 25-I-8°.

(2) Cnil, Délib. 2016-037 du 18-2-2016.
(3) Une troisième catégorie regroupe les éléments que la personne connaît, tels que par exemple un mot de passe.
(4) Loi 78-17 du 6-1-1978, art. 7.

Point sur le périmètre autorisé de la biométrie au travail

 La Cnil a publié plusieurs décisions sur l'usage de la biométrie dans le milieu du travail durant l'année 2015.

C'est l'occasion de revenir sur le périmètre autorisé de cet usage. Parce qu'elle permet l'identification d'une personne par ses caractéristiques physiques, biologiques voire comportementales, la biométrie est considérée comme une technologie particulièrement sensible au regard de la règlementation Informatique et libertés et son usage est soumis à une autorisation préalable de la Cnil.

Finalités autorisées par la Cnil – Concernant l'utilisation de la biométrie sur les lieux de travail, la Cnil a défini dans plusieurs autorisations uniques (1) les finalités pour lesquelles elle autorisait le recours à cette technologie. Il s'agit :

- des traitements mis en œuvre par des organismes privés ou publics reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail (Autorisation unique n° AU-007) ;
- des dispositifs biométriques mis en œuvre par des organismes privés ou publics reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail (Autorisation unique n° AU-008) ;
- des traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire, mis en œuvre par des établissements publics locaux d'enseignement du second degré et des établissements privés d'enseignement du second degré (Autorisation unique n° AU-009).

Dans quatre décisions rendues le 15 octobre 2015 (2), la Cnil a autorisé la mise en place de dispositifs biométriques à des fins de contrôle de l'accès aux locaux professionnels identifiés comme sensibles, validant à nouveau le principe du recours à la biométrie pour cette finalité.

Finalités rejetées par la Cnil – En revanche, dans cinq décisions rendues entre mars et juin 2015 (3), la Cnil a refusé d'autoriser la mise en place de dispositifs biométriques à des fins de suivi et de contrôle des horaires des salariés.

Historiquement, le champ d'application de l'autorisation unique n° AU-007 couvrait pourtant la gestion des horaires du personnel. En 2012, cette finalité a toutefois été exclue, la Cnil considérant désormais la biométrie comme un moyen disproportionné d'atteindre une finalité de contrôle des horaires.

Saisie de demandes d'autorisation par des entreprises souhaitant utiliser la biométrie à des fins de suivi et contrôle des horaires, la Cnil a eu l'occasion de réaffirmer sa position à plusieurs reprises en 2013, en 2014 et également en 2015.

Dans les cinq délibérations précitées, la Cnil a indiqué que toute demande d'autorisation pour l'installation d'un dispositif biométrique devait « s'inscrire dans le cadre de circonstances exceptionnelles fondées sur un impératif spécifique de sécurité (…) qui seraient susceptibles de justifier, notamment, la proportionnalité du recours à un dispositif biométrique ».

La simplification de l'identification du collaborateur, la possibilité de palier aux oublis et pertes de badges, la vérification de l'identité du collaborateur ayant pointé ou la possibilité de minimiser les risques d'erreur notamment sont autant de raisons refusées par la Cnil pour justifier le recours à la biométrie sur les lieux de travail.

Techniques biométriques – Dans les décisions de 2015 rendues à propos du suivi et contrôle des horaires des salariés, les dispositifs envisagés étaient basés sur la reconnaissance du contour de la main ou celle des empreintes digitales des salariés.

Dès lors que la finalité revendiquée apparaissait disproportionnée aux yeux de la Cnil, peu importait que le système utilisé soit :

- un dispositif "à trace" tel que la reconnaissance de l'empreinte digitale ou ;
- un dispositif sans trace tel que la reconnaissance du contour de la main, ces dispositifs présentant pourtant des risques moindres en termes d'usurpation d'identité, dans la mesure où les caractéristiques biométriques utilisées peuvent plus difficilement être capturées à l'insu d'une personne.

En revanche, dans les quatre décisions rendues le 15 octobre 2015, la Cnil a autorisé la mise en place de dispositifs biométriques multimodaux à des fins de contrôle de l'accès aux locaux professionnels. La particularité des dispositifs présentés résidait dans le recours à des dispositifs biométriques bimodaux, fondés à la fois sur la reconnaissance de l'empreinte digitale et du réseau veineux d'un individu et permettant ainsi d'améliorer les performances du dispositif.

Synthèse – En dehors des finalités de contrôle d'accès aux locaux et à la restauration validés par la Cnil notamment dans le cadre de ses autorisations uniques, l'installation de dispositifs biométriques sur les lieux de travail doit répondre à un impératif spécifique de sécurité.

La démonstration des circonstances exceptionnelles justifiant le recours à la biométrie pourrait alors passer par la réalisation d'une analyse d'impact justifiant le recours à cette technologie en réponse à un risque particulier qui aurait été identifié.

La technique biométrique utilisée et son niveau de performance pourront alors être mis en avant afin de justifier la proportionnalité du recours à cette technologie.

Alain Bensoussan Avocats
Lexing, Droit Informatique et libertés

(1) Afin de simplifier les formalités préalables pour les responsables de traitement, la Cnil a adopté plusieurs autorisations uniques, décrivant chacune des traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires. Un organisme souhaitant mettre en place un dispositif biométrique qui serait couvert en tous points par l'une des autorisations uniques de la Cnil n'a alors qu'à adresser à la Cnil un engagement de conformité à cette autorisation unique. En revanche, si le dispositif envisagé n'est pas couvert par une autorisation unique, le responsable du traitement doit adresser à la Cnil une demande d'autorisation spécifique décrivant le dispositif en cause.
(2) Délib. 2015-363 du 15-10-2015 ; Délib. 2015-361 du 15-10-2015 ; Délib. 2015-362 du 15-10-2015 ; Délib. 2015-360 du 15-10-2015.
(3) Délib. 2015-176 du 11-6-2015 ; Délib. 2015-141 du 7-5-2015 ; Délib. 2015-140 du 7-5-2015 ; Délib. 2015-087 du 5-3-2015 ; Délib. 2015-088 du 5-3-2015.

Biométrie en milieu scolaire : La Cnil rappelle les limites


La Cnil a refusé la mise en place d'un dispositif de biométrie en milieu scolaire consistant en la reconnaissance du réseau veineux des doigts de la main.

La Commission rappelle que « les données biométriques ne sont pas des données à caractère personnel comme les autres » et qu'elles représentent des risques particuliers au regard de la vie privée et des libertés individuelles.

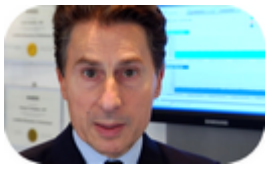
A l'inverse du contour de la main, qui est considéré comme une donnée « peu identifiante » et qui a fait l'objet d'une autorisation de la Cnil en 2006, le réseau veineux du doigt constitue « une technique biométrique plus précise et plus fiable qui n'évolue pas dans le temps et qui permet d'identifier a priori la personne concernée tout au long de sa vie », souligne la Cnil.

En conséquence, si la base de données de réseau veineux était détournée, « elle pourrait faire peser un risque sérieux sur l'intégrité et la protection des données biométriques des élèves » conclut la Cnil.

La Commission a estimé, au regard des risques existants et de la nature de la population concernée (élèves mineurs), que le dispositif biométrique envisagé était disproportionné par rapport au but recherché (améliorer la gestion de la cantine scolaire). Elle a, en outre, souligné que la gestion des accès à la cantine pouvait être réalisée par d'autres moyens comme un badge remis à chaque utilisateur ou le recours à la biométrie du contour de la main.

Cnil, rubrique Actualité, article du 30 novembre 2011

Aspects juridiques de la biométrie


Dans son rendez-vous bimestriel accordé à MyDSI-Tv, Maître Alain Bensoussan, présente les aspects juridiques de la biométrie de sécurité.

Qu'il s'agisse de la biométrie de sécurité à usage professionnel ou de confort, la biométrie, technologie nouvelle, est déjà régulée par le droit…

Emission du 30-9-2011, MyDSI-Tv, le média des DSI créé par Accenture.

Autorisation d'un dispositif de biométrie comportementale


Par une délibération en date du 23 juin 2011, la Cnil a autorisé, pour la première fois, un dispositif de biométrie comportementale.

L'autorisation concerne l'utilisation de la reconnaissance de la frappe du clavier comme dispositif biométrique, afin de renforcer l'identification d'une personne et lui permettre l'accès à un système d'information.

Ce dispositif requérant l'enregistrement de données à caractère personnel tels le nom, le prénom, le pseudonyme et l'adresse IP, il est soumis aux dispositions de l'article 25-I-8° de la loi du 6 janvier 1978 qui subordonne son utilisation à l'autorisation de la Cnil.

Cette autorisation de biométrie comportementale intervient dans un périmètre strictement défini par la Cnil, à savoir pour la démonstration prévue auprès de clients. Elle est encadrée par des règles de sécurité strictes afin de conserver la confidentialité des données.

Cnil, Délib. n° 2011-183 du 23-6-2011

La CNIL autorise le recours à la biométrie comme moyen de paiement

La Cnil, fidèle à sa ligne de conduite, a autorisé un nouveau système de paiement biométrique sans trace.

Contrairement à une empreinte digitale classique, l'empreinte veineuse ne peut être collectée, ce qui limite une usurpation d'identité presque « *parfaite* ».En tête des systèmes de biométrie, la reconnaissance du réseaux veineux permet aux consommateursde s'authentifier à l'aide de leur doigt pour faire leurs achats.

Ce procédé consiste à approcher un doigt du terminal de paiement (TPE), muni d'un capteur infrarouge qui « *photographiera* » les veines du doigt pour les comparer, par ondes radio chiffrées et sécurisées, à un gabarit enregistré dans une carte bancaire.

Ce dispositif ouvre la voie à de nouvelles attitudes, la manipulation de la carte devenant inutile. Le vol de carte apparaît, dès lors, sans grand intérêt et les codes oubliés risquent de devenir de mauvais souvenirs. Si cette technologie est ainsi proportionnée et conforme aux préconisations de la Cnil en matière de biométrie, elle reste un test d'une durée de six mois, qui donnera lieu à un bilan avant de toucher, semble t-il, un large public.

Cnil, Communiqué du 1-4-2010

La biométrie sur le lieu de travail autorisée par la Cnil

 Biométrie sur le lieu de travail autorisée par la Cnil

La Cnil a adopté une autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur le lieux de travail. Elle considère que la gestion des contrôles de l'accès physique à l'entrée des lieux de travail et dans les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation, peut s'effectuer grâce à la biométrie.

Cnil, Autorisation unique AU-019 du 7-5-2009

Paru dans la JTIL n°29/2009 p.5

(Mise en ligne Septembre 2009)

La biométrie fait son entrée dans l'entreprise

La biométrie fait son entrée dans l'entreprise : la Cnil rappelle les règles

La Cnil rappelle que son autorisation est obligatoire pour la mise en œuvre de traitements comportant des données biométriques (reconnaissance de la rétine, du contour de la main, de l'empreinte. La sécurité est un marché en plein essor dans lequel de nombreux éditeurs de solutions se sont engouffrés, proposant aux entreprises des dispositifs de reconnaissance des empreintes digitales. Face à ce développement, la Cnil a tenu à effectuer une mise au point : aucun dispositif biométrique n'a fait l'objet d'un « label CNIL » ou d'un agrément a priori. D'une manière générale, la Cnil n'autorise que les dispositifs où les données biométriques comme les empreintes digitales sont enregistrées exclusivement sur un support individuel (carte à puce, clé USB) et non dans une base de données

centralisée.

Communiqué de la Cnil du 05/1/2007

(Mise en ligne Janvier 2007)

Biométrie allégée pour la reconnaissance du réseau veineux palmaire


Vidéosurveillance, géolocalisation et biométrie font désormais partie de la panoplie sécuritaire des espaces privés ou publics. Aujourd'hui, l'accès à une salle d'examen ou un bloc opératoire peut ainsi être soumis à l'obligation de scanner le réseau veineux palmaire du candidat ou du personnel médical (1). En application de la loi Informatique et libertés, modifiée en 2004, les dispositifs de reconnaissance biométrique sont, pour la plupart, soumis à une autorisation préalable de la Cnil. Or, la Cnil vient d'alléger les formalités d'autorisation, pour la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main, privilégiant ainsi les dispositifs d'identification sans contact (2). Encore faut-il que cette technique ne soit affectée qu'au contrôle d'accès des locaux sur le lieu de travail. La société qui souhaite s'équiper d'un tel dispositif dans le respect des dispositions de la décision unique n°AU-019, doit adresser à la Cnil un engagement de conformité. La biométrie regroupe les techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Ces données sont ainsi considérées comme des données à caractère personnel, permettant d'identifier une personne de manière irrévocable. Or, tous les traitements comportant des données biométriques doivent faire l'objet d'une autorisation préalable de la Cnil.

Parmi les données biométriques utilisées aujourd'hui, la Cnil considère l'empreinte digitale comme une donnée à risque, dont la diffusion, non maîtrisée ou accidentelle, peut avoir des conséquences irrémédiables pour les personnes. Contrairement à tout autre identifiant (code, mot de passe), l'empreinte digitale ne peut être modifiée une fois collectée, ce qui impose d'en limiter l'usage pour éviter une usurpation d'identité presque « *parfaite* ». Cette « *biométrie à trace* » est donc particulièrement encadrée par la Cnil qui, l'an dernier, a refusé d'autoriser plusieurs dispositifs ne pouvant justifier d'un fort impératif de sécurité. Pour la Cnil, confier ses données biométriques à un tiers doit répondre à une nécessité exceptionnelle et être entourée de garanties sérieuses. Cette technologie doit, tout d'abord, présenter certaines caractéristiques techniques (chiffrage de l'enregistrement du gabarit veineux ou possibilité d'associer d'autres données d'identification – nom, prénom, photographie – au gabarit du réseau veineux du doigt). La durée de conservation des données doit être fixée

(de 3 mois à 5 ans selon les cas). Le responsable du traitement doit également prendre « *toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance* » (3). Enfin, l'information des employés et des instances représentatives du personnel doit être effectuée avant la mise en œuvre effective du dispositif biométrique, sous peine d'une peine pouvant atteindre 300 000 euros d'amende et 5 ans de prison.

(1) Cnil, Délib. 2009-360 du 18-06-2009 et 2009-174 du 26-03-2009
(2) Cnil, Délib. 2009-316 du 07-05-2009
(3) Loi du 06-01-1978 modifiée, art 34

La biométrie sur le lieu de travail autorisée par la Cnil

Informatique et libertés

Biométrie

Biométrie sur le lieu de travail autorisée par la Cnil

La Cnil a adopté une autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur le lieux de travail. Elle considère que la gestion des contrôles de l'accès physique à l'entrée des lieux de travail et dans les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation, peut s'effectuer grâce à la biométrie.

Cnil, Autorisation unique AU-019 du 7-5-2009

Paru dans la JTIL n°29/2009 p.5

(Mise en ligne Septembre 2009)

La Cnil autorise la biométrie pour lutter contre la fraude

Informatique et libertés

Biométrie

La CNIL autorise la biométrie pour lutter contre la fraude

La Cnil vient de publier un communiqué dans lequel elle indique qu'elle a autorisé, lors de sa séance plénière du 18 juin 2009 (cette délibération n'a pas encore été publiée), le recours à un traitement de données à caractère personnel fondé sur la reconnaissance du réseau veineux de la paume de la main des candidats à un examen. Ce traitement serait destiné à lutter contre la fraude à l'examen du GMAT (Graduate Management Admission Test), un examen de gestion et de management permettant d'évaluer les compétences des candidats pour intégrer certaines grandes écoles dans le monde entier. Deux arguments principaux ont emporté l'adhésion de la Cnil à la mise en œuvre de ce système biométrique :

– la technologie utilisée qui constitue selon la Cnil une biométrie « sans trace » et présente des risques particulièrement réduits d'usurpation d'identité ;
– les particularités de l'examen concerné par ce traitement, notamment sa dimension mondiale, les enjeux qui y sont attachés et l'existence de nombreuses fraudes dans le passé.

La Cnil tempère toutefois les conséquences de cette décision, précisant qu'elle n'est pas favorable à l'utilisation systématique de dispositifs biométriques pour lutter contre la fraude aux examens d'une manière générale.

Communiqué Cnil du 15 juillet 2009.

(Mise en ligne Juillet 2009)