la Cnil encadre l'usage des données biométriques dans les entreprises et les administrations

Entreprises et administrations françaises adoptent de plus en plus les techniques de la biométrie pour une identification rapide et efficace des personnes. Cependant elles mettent en jeu des données personnelles à manier avec précaution. La Commission nationale de l'informatique et des libertés apporte sa protection.

1. autorisation de la Cnil

Les dispositifs biométriques regroupent l'ensemble des techniques qui permettent d'identifier une personne à partir d'une caractéristique physique : l'ADN, la rétine, l'iris, l'empreinte digitale, l'empreinte palmaire, la reconnaissance du réseau veineux du doigt, la reconnaissance faciale, la géométrie du contour de la main, la voix, l'écriture... Or, celles-ci peuvent porter atteinte aux droits fondamentaux s'il en résulte une surveillance généralisée des individus qui pourrait permettre de tracer chacun dans le monde réel.

Aussi la loi du 6 août 2004 soumet-elle tous les dispositifs de traitements de données biométriques à l'autorisation de la Cnil et le nombre de demandes d'autorisation pour de tels systèmes ne cesse d'augmenter.

La Cnil a admis que certains dispositifs de biométrie puissent bénéficier de formalités allégées, ne nécessitant qu'une simple déclaration de conformité en ligne à une autorisation unique émise par elle. C'est dans ces conditions qu'ont été autorisés :

- des dispositifs de reconnaissance du contour de la main (pour l'accès à un restaurant scolaire ou à des lieux de travail) (1, 2)...
- des dispositifs de reconnaissance du réseau veineux des doigts de la main (pour le contrôle d'accès à des lieux de travail) (3) ;
- des dispositifs reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée (carte à puce ou clé USB par exemple pour le contrôle d'accès à des locaux...) (4).

Par une délibération du 20 septembre 2012 (5), la Cnil a considéré que les horaires des salariés ne pouvaient plus être contrôlés par un dispositif biométrique.

avec ou sans traces

Plus généralement, la Cnil fait preuve d'une grande prudence à l'égard des technologies biométriques, opérant une distinction entre les technologies dites « *avec traces* » et celles dites « *sans traces* ». Est considéré comme biométrie « *avec traces* », le dispositif qui permet de « *récupérer* » l'élément identifiant à l'insu de la personne. Ainsi en est-il d'une empreinte digitale qui peut par exemple être récupérée sur le verre qu'un individu aura tenu en main. La biométrie « *sans trace* » ne permet pas, à l'inverse, de capturer et de copier des éléments identifiants, à l'insu de la personne concernée.

2. critères de la Cnil

La Cnil juge de la légitimité du dispositif biométrique mis en œuvre au regard de ses propres critères.

■ 1er critère : finalité du dispositif

Le dispositif doit être limité au contrôle de l'accès à une zone bien définie pour un nombre déterminé de personnes, et ce, afin de protéger l'intégrité de personnes, de biens et d'installations, ou d'informations.

Il n'y a pas de difficulté, en principe, à obtenir de la Cnil des autorisations pour des dispositifs biométriques reposant sur la reconnaissance du contour de la main ou lorsque le gabarit de l'empreinte digitale est stocké dans un support individuel (carte à puce, clé USB) et non dans une base de données centralisée (par exemple, un terminal de lecture-comparaison ou un serveur). La Cnil considère que ces technologies de reconnaissance biométrique

présenteraient un danger moindre, car elles ne laissent pas de traces susceptibles d'être captées à l'insu de la personne et d'être utilisées à des fins étrangères à la finalité initiale assignée au dispositif. Aucune image n'est conservée, seule la clé biométrique, résultat du traitement des mesures par un algorithme, est associée à l'identité de la personne.

du Musée du Louvre à un CHU

C'est au regard de ces critères que la Cnil a autorisé à plusieurs reprises la mise en place de dispositifs de reconnaissance de la morphologie de la main (pour le Musée du Louvre, ou encore pour accéder à une cantine scolaire) (6, 7). Elle a également autorisé des dispositifs d'empreintes digitales pour l'accès à des zones hautement sécurisées (notamment pour la Banque de France ou encore pour contrôler l'accès aux zones de sûreté des aéroports d'Orly et de Roissy) (8, 9). Elle a encore autorisé l'utilisation d'un dispositif d'accès par empreintes digitales pour un bloc opératoire dans un CHU confronté à des problèmes spécifiques d'intrusion liés au voisinage. On peut ainsi imaginer qu'un tel système soit utilisé afin de permettre un accès informatisé sécurisé des médecins aux dossiers médicaux de leurs patients. Elle a également autorisé le contrôle de l'accès à des postes informatiques portables professionnels (10).

2e critère : proportionnalité

Le dispositif doit être proportionné à la finalité préalablement définie, à raison des risques qu'il comporte en matière de protection des données à caractère personnel. Il doit être limité au contrôle de l'accès d'un nombre défini de personnes à une zone bien déterminée, représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme tel que la protection de l'intégrité physique des personnes, de celle des biens et des installations ou encore de celles de certaines informations (par exemple, l'accès à une centrale nucléaire ou encore à une cellule de vaccins). Il ne peut être installé que dans les cas où il est adapté aux risques encourus. Ainsi, si une solution alternative existe (par exemple : badge, RFID sans données biométriques), elle doit être privilégiée.

La Cnil a ainsi rendu des avis défavorables pour la mise en place de dispositifs biométriques pour accéder à une cantine scolaire (11) ou à des locaux professionnels (12). Dans les cas visés, elle a considéré que la conservation des données biométriques permettait leur détournement à des fins étrangères à la finalité poursuivie, notamment à fin d'identification d'une personne à partir d'objets les plus divers qu'on a pu toucher ou avoir en main.

3e critère : sécurité

Des garanties doivent être prises pour que le dispositif permette à la fois une authentification ou une identification fiable des personnes et comporte toutes garanties de sécurité pour éviter la divulgation des données.

L'appréciation de la Cnil est sévère, comme l'illustre l'avis défavorable qu'elle a émis à la mise en place d'un dispositif de lecture de badges et d'empreintes digitales voulu par une préfecture, considérant que la constitution d'une base de données biométriques ne se justifiait pas, l'identification par badge étant suffisante selon elle pour répondre à l'impératif de sécurité recherché. De même, elle a délivré un avis défavorable à la mise en place, par un centre hospitalier, d'un dispositif de reconnaissance de l'empreinte digitale utilisé pour le contrôle des temps de travail des agents, considérant que les données biométriques étaient stockées non pas sur un support individuel, mais dans un lecteur biométrique sur lequel l'employé n'avait aucune maîtrise (13). Elle a encore refusé d'accorder à une banque l'autorisation de mettre en œuvre un traitement automatisé de données personnelles reposant sur un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle et le suivi du temps de travail au motif que le traitement envisagé ne relevait pas d'une finalité de sécurité justifiant un recours impératif à la biométrie et qu'il n'apparaissait *« ni adapté, ni proportionné à la finalité poursuivie »* (14).

4e critère : l'information des personnes concernées

Elle doit se faire à la fois dans le respect de la loi informatique et liberté et du Code du travail. On retiendra, à titre de règle générale, que les personnes concernées doivent toujours être individuellement informées de la mise en œuvre des dispositifs biométriques, des modalités de leur droit d'accès aux données et de la finalité des mesures de contrôle.

La cour d'appel de Paris a rappelé l'obligation d'information des salariés concernés par la mise en œuvre d'un dispositif de collecte d'information biométriques dans un arrêt du 21 mai 2015 (15). ■

Christiane Féral-Schuhl
[Avocate associée, ancien bâtonnier de Paris]

(1) Cnil, Autorisation unique n° AU-009 - Délibération n° 2006-103 du 27 avril 2006 :
→ www.cnil.fr/documentation/deliberations/deliberation/delib/103/
(2) Cnil, Autorisation unique n ° AU-007, Délibération n° 2006-101 du 27 avril 2006 :
→ www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000813778&dateTexte=
(3) Cnil, Autorisation unique n° AU-019, Délibération n° 2009-316 du 7 mai 2009 :
→ www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020764858
(4) Cnil, Autorisation unique n° AU-008 - Délibération n° 2006-102 du 27 avril 2006 :
→ www.cnil.fr/documentation/deliberations/deliberation/delib/104/
(5) Cnil, Autorisation unique n° AU-007 - Délibération n° 2012-322 du 20 septembre 2012 : ■■■■

■■■■
→ www.cnil.fr/documentation/deliberations/deliberation/delib/105/
(6) Cnil, Délibération n° 01-006, 25 janv. 2001 :
→ www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653393
(7) Cnil, Délibération n° 02-070 du 15 octobre 2002 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653623&fastReqId=1210188817&fastPos=1
(8) Cnil, Délibération n° 97-044 du 10 juin 1997 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653121&fastReqId=31588235&fastPos=1
(9) Cnil, Délibération n° 04-017 du 8 avril 2004 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653148&fastReqId=157693680&fastPos=1
(10) Cnil, Autorisation unique n ° AU-027 - Délibération n° 2011-074 du 10 mars 2011 :
→ www.cnil.fr/documentation/deliberations/deliberation/delib/254/
(11) Cnil :
→ www.cnil.fr/linstitution/actualite/article/article/biometrie-la-cnil-refuse-lutilisation-du-reseau-veineux-dans-une-cantine-scolaire/
(12) Cnil, Délibération n° 2008-216 du 17 juillet 2008 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000019796279&fastReqId=952561112&fastPos=1
(13) Cnil, Délibération n° 04-018 du 8 avril 2004 :
→ www.cnil.fr/documentation/deliberations/deliberation/delib/56/
(14) Cnil, Délibération n° 2015-087 du 5 mars 2015 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000030481101&fastReqId=1036919625&fastPos=1
(15) Arrêt de la Cour d'appel de Paris, N° Répertoire général : 12/12029 du 21 mai 2015.

⊞ repères

cas pratiques

■ autorisation pour un dispositif reposant sur la reconnaissance vocale

La Cnil a autorisé la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion et la réinitialisation des mots de passe utilisés pour accéder au système d'information de la société (*). Le procédé repose sur la reconnaissance du gabarit de l'empreinte de la voix des employés. Il prévoit que, lors de la procédure d'enrôlement, l'employé procédera à l'enregistrement du gabarit de son empreinte vocale grâce à la répétition de plusieurs couples de prénoms choisis aléatoirement parmi plus de 4 000 combinaisons possibles. Pour réinitialiser leur mot de passe informatique, les employés appelleront un serveur vocal. Lors de la réinitialisation d'un mot de passe, le dispositif procédera à une comparaison entre les mots répétés par l'utilisateur au profil de référence, c'est-à-dire au gabarit de l'empreinte vocale de la personne. Une fois que l'utilisateur a été correctement authentifié, l'application réinitialise le mot de passe et le communique à l'utilisateur. Les données seront conservées le temps de l'existence du compte informatique de l'employé.

adapté et proportionné

Compte tenu des modalités de mise en œuvre du dispositif et notamment des moyens utilisés pour garantir la sécurité des données et prévenir tout risque d'usurpation d'identité ou d'utilisation des données pour d'autres finalités, la Cnil a considéré que le recours à la constitution d'une base de données de gabarit d'empreintes vocales aux fins de gérer les mots de passe informatique est adapté et proportionné à la finalité assignée au dispositif, au regard de la protection des données personnelles.

■ dispositif de reconnaissance du réseau veineux

Plus récemment, la Cnil a autorisé le recours à un système biométrique reposant sur la reconnaissance du réseau veineux pour lutter contre la fraude à un examen. La Cnil a justifié sa décision en se fondant à la fois sur la particularité de l'examen (examen international d'accès à des grandes écoles pour lequel des contrôles particulièrement exigeants sont indispensables) et sur la fiabilité du dispositif (analyse de l'image du réseau veineux à l'intérieur de la paume de la main) qualifié par la Cnil de dispositif « *sans trace* » (**).
En revanche, la Cnil a refusé la mise en place d'un dispositif biométrique basé sur la reconnaissance du réseau veineux des doigts de la main dans une cantine scolaire d'un collège. Ce dispositif avait pour but de débloquer le plateau de la cantine, de tenir la comptabilité et de suivre les passages des utilisateurs (***). ■

(*) Cnil, délibération n° 2007-248 du 13 septembre 2007 :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017652004&fastReqId=1413805300&fastPos=1
(**) Cnil, Délibération n° 2009-360 du 18 juin 2009 :
→ legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000020972764&fastReqId=1757624634&fastPos=2
(***) Cnil, Délibération n° 2011-147 du 19 mai 2011, Légifrance :
→ www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000024880869&fastReqId=1821005304&fastPos=2