

Commission nationale de l'informatique et des libertés

Délibération n° 2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)

NOR : CNIL1626008X

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu le code du travail, notamment ses articles L. 1222-4, L. 2143-22, L. 2315-5, L. 2323-13 et suivants, L. 2323-32, L. 2325-11 et L. 8113-4 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment ses articles 25-I (8°) et 25-II ;

Vu la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Vu la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat ;

Vu la loi n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu le décret n° 82-452 du 28 mai 1982 relatif aux comités techniques paritaires ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels ;

Vu la délibération n° 2009-316 du 7 mai 2009 portant 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 les lieux de travail ;

Vu la délibération n° 2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques 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 ;

Vu la délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements 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 ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Les données biométriques ont la particularité d'être uniques et permanentes, car elles permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (ex. : empreinte digitale, contour de la main). Elles ne sont pas attribuées par un tiers ou choisies par la personne. Elles sont produites par le corps lui-même et le désigne de façon définitive. Elles permettent de ce fait le suivi des individus et leur identification.

La gestion des contrôles de l'accès à des zones, appareils et applications limitativement identifiées par le responsable de traitement comme faisant l'objet d'une restriction de circulation et d'accès peut s'effectuer grâce à la mise en œuvre d'un dispositif de reconnaissance biométrique résultant d'un traitement technique spécifique des caractéristiques physiques, physiologiques ou comportementales d'une personne physique, permettant ou confirmant son identification unique, telles que des images faciales ou des données dactyloscopiques.

Le caractère sensible des données issues de ce traitement justifie que la loi prévoit un contrôle spécifique de la CNIL, pour apprécier la proportionnalité du traitement au regard de la finalité recherchée telle que la gestion des restrictions d'accès mises en place dans un contexte professionnel. De tels dispositifs relèvent en effet de l'article 25-I (8°) de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Par ailleurs, il y a lieu, en l'état des connaissances sur la technologie utilisée, de faire application des dispositions de l'article 25-II aux termes duquel les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et les mêmes destinataires ou catégories de destinataires, peuvent être autorisés par une décision unique de la commission. Au cours des dernières années, la commission a émis plusieurs autorisations uniques de mise en œuvre de dispositifs biométriques de contrôle d'accès aux lieux de travail fondés soit sur la reconnaissance du contour de la main (délibération n° 2006-101 du 27 avril 2006 portant autorisation unique 007), soit sur la reconnaissance de l'empreinte digitale (délibération n° 2006-102 du 27 avril 2006 portant autorisation unique 008), soit sur la reconnaissance du réseau veineux des doigts de la main (délibération n° 2009-316 du 7 mai 2009 portant autorisation unique 019), ou de contrôle d'accès aux postes informatiques portables professionnels par reconnaissance de l'empreinte digitale (délibération n° 2011-074 du 10 mars 2011 portant autorisation unique 027).

Les dispositifs autorisés par ces décisions uniques ont pour finalité commune la gestion et le contrôle des restrictions d'accès définies dans un contexte professionnel, que ces accès soient logiques ou physiques, à partir de différentes caractéristiques biométriques. Toutefois, les modalités de conservation du gabarit qu'elles autorisent diffèrent en fonction des caractéristiques biométriques utilisées.

L'évolution des technologies appelle une révision des cadres de références actuels.

Face au développement du recours aux dispositifs biométriques aux fins de contrôle d'accès, la commission doit veiller, conformément à l'article 1^{er} de la loi du 6 janvier 1978 modifiée, à ce que ces traitements restent au service du citoyen et ne « portent atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

La délibération n° 2016-186 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique, pose des conditions garantissant un haut niveau de confidentialité et une limitation des risques de détournement ou d'usurpation de la donnée. Dès lors, la commission appelle les responsables du traitement à privilégier les dispositifs biométriques répondant aux conditions édictées par cette délibération de manière à préserver la maîtrise des personnes sur leurs données biométriques.

Toutefois, la détention d'un support de stockage ou d'un secret par la personne concernée n'est pas toujours compatible avec les besoins du responsable du traitement et avec le contexte de mise en œuvre du dispositif biométrique. La conjugaison de plusieurs facteurs, tels que le nombre de personnes concernées, les exigences sanitaires applicables aux locaux protégés, leur sensibilité ou encore la nécessité pour le responsable du traitement de maîtriser en temps réel l'ensemble du dispositif, peut contribuer à justifier un stockage des gabarits en base centrale interconnectée aux différents terminaux de lecture comparaison ou sur le serveur de ces derniers.

Afin de tenir compte de ces situations, la présente décision précise les conditions de mise en œuvre des traitements biométriques reposant sur une conservation des gabarits en base par le responsable du traitement. Ces conditions portent tant sur la justification de la pertinence de ces dispositifs que sur les mesures à mettre en œuvre pour limiter les risques de détournement et d'usurpation de la donnée et plus généralement les risques pour la vie privée des personnes concernées.

Le périmètre des traitements biométriques couverts par la présente autorisation unique s'étend à toute personne disposant d'une habilitation d'accès contrôlée par le dispositif biométrique mis en œuvre par le responsable du traitement concerné, et à toute caractéristique biométrique, utilisée seule ou de manière combinée. Enfin, la présente autorisation ne vise pas un type de local ou d'appareil précis mais, de manière plus générale, tout local, appareil ou application identifié de manière limitative par le responsable du traitement comme faisant l'objet d'une restriction d'accès par contrôle d'accès biométrique.

Le responsable de traitement mettant en œuvre un dispositif de contrôle d'accès reposant sur la reconnaissance d'une des caractéristiques biométriques visées par la présente décision dans le respect de ses dispositions adresse à la commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation. Il s'engage à documenter les mesures prises pour répondre à chacune des dispositions de la présente autorisation.

Dès lors, les responsables de traitement qui adressent à la commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Art. 1^{er}. – *Finalités du traitement.*

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente décision unique les traitements reposant sur un dispositif de reconnaissance d'une caractéristique biométrique, mis en œuvre par les organismes privés ou publics, à l'exception des traitements mis en œuvre :

- pour le compte de l'Etat ;
- lorsque les personnes concernées sont des mineurs.

Ces traitements peuvent uniquement avoir pour finalité :

- le contrôle des accès à l'entrée et dans les locaux limitativement identifiés par l'organisme comme devant faire l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés ;
- le contrôle des accès à des appareils et applications informatiques professionnels limitativement identifiés de l'organisme, à l'exclusion de tout contrôle du temps de travail de l'utilisateur.

Toutefois, le responsable du traitement s'engage à justifier au moyen d'une documentation appropriée :

- du choix de recourir à un dispositif biométrique plutôt qu'à un traitement non biométrique au regard de la finalité du traitement ;
- du choix du stockage des gabarits en base et des contraintes faisant obstacle au maintien de la maîtrise individuelle des personnes sur leur gabarit.

Art. 2. – Données à caractère personnel traitées.

Seules les données à caractère personnel suivantes peuvent être traitées :

- l'identité : nom, prénom, photographie et gabarit de la caractéristique biométrique, clé biométrique résultat du traitement des mesures par un algorithme (et non une image ou une photographie de cette caractéristique), numéro d'authentification ou numéro de support individuel, coordonnées ;
- la vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade, nom de l'employeur ;
- le déplacement des personnes : porte utilisée, zones et plage horaire d'accès autorisées, date et heure d'entrée et de sortie ;
- en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement.

Art. 3. – Modalités et durée de conservation.

Les caractéristiques biométriques ne peuvent être conservées que sous la forme d'un gabarit chiffré ne permettant pas de recalculer la donnée biométrique d'origine, soit en base de données où elles peuvent être associées à un numéro d'authentification de la personne, soit dans la mémoire interne du terminal de lecture comparaison qui ne dispose d'aucun port de communication permettant l'extraction de ce gabarit.

Le gabarit de la donnée biométrique ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ.

Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent être conservées au maximum cinq ans après le départ de la personne disposant d'une habilitation d'accès de longue durée, et trois mois après le départ des personnes disposant d'une habilitation d'accès ponctuelle.

Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de trois mois.

Art. 4. – Destinataires des informations.

Personnes habilitées du service du personnel	Identité (à l'exception du gabarit de la biométrie utilisé et du code d'authentification), vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking
Personnes habilitées du service gérant la sécurité des locaux	Identité (à l'exception du gabarit de la biométrie utilisée et du code d'authentification), plages horaires autorisées, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking ou des locaux
Personnes habilitées du service ou de l'organisme gérant le restaurant d'entreprise ou administratif	Identité (à l'exception du gabarit de la biométrie utilisée et du code d'authentification), informations en relation avec la gestion de la restauration

Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit de l'empreinte digitale que de façon temporaire et pour les stricts besoins de l'enrôlement de la personne concernée ou de la suppression du gabarit, sans qu'il leur soit possible d'accéder directement, de modifier, ou de copier sur un autre support, les gabarits enregistrés.

Art. 5. – Liberté de circulation des employés protégés.

Les contrôles d'accès aux locaux du responsable de traitement et aux zones limitativement désignées, faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent, ne doivent pas entraver la liberté d'aller et venir des employés protégés dans l'exercice de leurs missions conformément aux dispositions du code du travail.

Art. 6. – Mesures de sécurité.

Le responsable du traitement prend toutes 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.

Compte tenu de la sensibilité des traitements concernées et des risques liés au stockage des gabarits en base, le responsable du traitement s'engage à documenter la conformité de son traitement sous forme d'analyse d'impact relative à la protection des données. L'analyse doit comprendre une description systématique des opérations de traitement envisagées et des finalités du traitement ainsi qu'une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, conformément à l'article 2 de la présente délibération. Elle doit également détailler les mesures envisagées afin de faire face aux risques pour les droits et libertés des personnes concernées, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel, conformément au présent article.

Au regard des risques identifiés par la commission, le responsable du traitement s'engage notamment à adopter les mesures suivantes, ou des mesures équivalentes dont il démontre l'équivalence :

- mesures portant sur les données :

- cloisonner les données lors de leur transmission et leur conservation ;
- chiffrer les données biométriques, dont les gabarits, à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art ; en particulier, une politique de chiffrement et de gestion des clés doit être clairement définie (changement des clés par défaut, algorithmes et tailles des clés conformes à l'état de l'art, renouvellement prévu...) ;
- associer un code d'intégrité aux données (par exemple, signature par hachage) ;
- interdire tout accès externe à la donnée biométrique (module de sécurité physique/logique type HSM) ;
- effectuer le contrôle d'accès par une comparaison entre l'échantillon calculé et le gabarit d'enrôlement enregistré (en base interne/distante) sans copie du gabarit ;
- veiller à l'effectivité de l'effacement des données à l'issue de la durée de conservation ;
- supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant ;
- supprimer toute donnée non utile au traitement ultérieur lors de la fin de vie du dispositif biométrique ;
- mesures portant sur l'organisation :
 - informer les personnes concernées, de manière complète, spécifique et intelligible, via des supports clairs et synthétiques ;
 - responsabiliser les personnes concernées sur les bonnes conditions d'utilisation des matériels ;
 - mettre à disposition un dispositif alternatif « de secours » ou utilisé à titre exceptionnel, sans contrainte ni surcoût pour les personnes n'utilisant pas la solution biométrique ; en particulier, pour les personnes ne répondant pas aux contraintes du dispositif biométrique (enrôlement ou lecture de la donnée biométrique impossible) et en prévision d'une indisponibilité du dispositif biométrique (tel qu'un dysfonctionnement du dispositif), une « solution de secours » doit être mise en œuvre pour assurer une continuité du service proposé, limitée toutefois à un usage exceptionnel ;
 - tester le système selon une procédure formalisée, avant sa mise en place et après toute modification, dans un environnement dédié et sans recourir à des données réelles ;
 - déterminer les actions à entreprendre en cas d'échec de l'authentification (impossible de vérifier une identité, défaut d'habilitation à pénétrer dans une zone sécurisée...) ;
 - gérer de manière stricte l'accès physique et logique aux dispositif et bases de données par les personnes habilitées ; en particulier, une politique de gestion des droits et des accès doit être clairement définie ; il s'agit de formaliser les différentes catégories de personnes habilitées (utilisateurs, administrateurs et gestionnaires de bases de données, personnes en charge de la gestion des données, personnes techniques de maintenance...), leurs droits sur les données, la manière dont les habilitations sont gérées, la manière dont leur accès est contrôlé, la manière dont les secrets sont gérés, les traces journalisées, la manière dont les traces sont gérées, etc. ;
 - former spécifiquement les administrateurs et personnes habilitées à gérer les données (enrôlement, traitements, effacement...) ;
 - intégrer une mesure technique ou organisationnelle de détection anti-fraude ;
 - prévenir les personnes concernées en cas d'accès non autorisé à leurs données ;
 - formaliser, appliquer et faire connaître une procédure de secours en cas d'incident (prévoyant notamment le ré-enrôlement) ;
 - obtenir un engagement de responsabilité de la part des administrateurs ;
 - journaliser les opérations effectuées sur les supports ;
 - assurer des mesures de sauvegarde ;
 - formaliser et tester une procédure de récupération du système ;
- mesures portant sur les matériels :
 - mettre en œuvre des mesures permettant d'être alerté en cas de tentative d'effraction sur le lecteur ou le dispositif de stockage ; en particulier, en cas de stockage de la donnée sur une base locale intégrée au dispositif biométrique, toute tentative d'ouverture ou d'arrachement du terminal de lecture/comparaison doit être détectée, suivie d'un signalement à l'administrateur du dispositif ;
 - réserver un matériel spécifique au stockage des données ;
 - utiliser des matériels certifiés aux conditions d'usage et en termes de sécurité ;
 - garantir la traçabilité du cycle de vie du matériel ;
- mesures portant sur les logiciels :
 - réserver un logiciel spécifique à l'usage des données ;
 - signer le logiciel et vérifier sa signature ;
 - tenir les logiciels à jour selon une procédure formalisée ;
 - vérifier que les modifications apportées par les éditeurs de logiciels ne favorisent pas la fuite de données ;
 - recourir à des mécanismes de détection et de protection contre les logiciels malveillants et logiciels espions, éprouvés et tenus à jour ;
 - limiter les actions des usagers sur les logiciels ;
 - garantir la traçabilité du cycle de vie des logiciels ;
 - vérifier régulièrement les licences des logiciels utilisés ;

- mesures portant sur les canaux informatiques :
 - sécuriser les canaux informatiques (canaux réservés et chiffrés) ;
 - interdire la transmission des gabarits stockés.

Le responsable du traitement s'engage à tenir à la disposition de la commission une copie de l'analyse d'impact relative à la protection des données établie en application du présent article.

Art. 7. – Information et droits des personnes.

L'information des personnes est effectuée, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée en août 2004, par la diffusion à chaque personne concernée, préalablement à la mise en œuvre du traitement, d'une note explicative.

La notice explicative précise notamment la manière d'exercer les droits d'accès, de rectification et d'opposition pour motif légitime.

Le responsable du traitement procède également, conformément aux dispositions des articles L. 2323-13 et suivants, L. 2323-32 du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre des traitements visés à l'article 1^{er}.

Art. 8. – Abrogation des délibérations n° 2011-074, n° 2009-316, n° 2006-102, n° 2012-322 et dispositions transitoires.

La délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique a abrogé la délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels, la délibération n° 2009-316 du 7 mai 2009 portant 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 les lieux de travail, la délibération n° 2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques 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 ainsi que la délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements 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.

Les organismes privés et publics ayant effectué un engagement de conformité à ces autorisations uniques et qui ne respectent plus les conditions fixées par la présente norme disposent d'un délai de deux ans à compter de la publication de la présente délibération pour mettre en conformité leur traitement avec la présente délibération ou la délibération n° 2016-186 adoptée ce jour ou demander une autorisation spécifique auprès de la commission dans les formes prescrites par les articles 25-8° et 30 de la loi du 6 janvier 1978 modifiée.

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance d'une caractéristique biométrique, qui n'est pas conforme aux dispositions qui précèdent, doit faire l'objet d'une demande d'autorisation auprès de la commission dans les formes prescrites par les articles 25 (8°) et 30 de la loi du 6 janvier 1978 modifiée.

Art. 9. – La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. FALQUE-PIERROTIN