

Commission nationale de l'informatique et des libertés

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

NOR : CNIA0900008X

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 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 son article 25 (8°) ;

Vu le code du travail, et 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° 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 ;

Sur le rapport de M. Didier Gasse et M. Hubert Bouchet, commissaires, et les observations de Mme Elisabeth Rolin, commissaire du Gouvernement ;

Formule les observations suivantes :

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 mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du réseau veineux des doigts de la main.

Dès lors, de tels dispositifs relèvent 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. 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.

Le responsable de traitement mettant en œuvre un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main dans le respect des dispositions de cette décision unique adresse à la commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation.

Décide que 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.

Article 1^{er}

Finalités et caractéristiques techniques 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 du réseau veineux des doigts de la main, 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 de l'organisme faisant l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés.

Le dispositif de reconnaissance du réseau veineux doit présenter les caractéristiques suivantes :

- seul le gabarit du réseau veineux du doigt, clé biométrique résultat du traitement des mesures par un algorithme, est enregistré et non une image ou une photographie du réseau veineux ;
- le gabarit du réseau veineux du doigt de la personne concernée est exclusivement enregistré sous une forme chiffrée soit dans la mémoire du terminal de lecture-comparaison qui ne dispose d'aucun port de communication permettant l'extraction de ce gabarit, soit sur un support individuel sécurisé qui reste en possession de la personne devant être authentifiée par le dispositif ;
- l'enrôlement des caractéristiques biométriques des personnes s'effectue exclusivement à partir du terminal de lecture-comparaison ;
- le contrôle d'accès s'effectue par une comparaison entre le doigt apposé sur le lecteur et le gabarit du réseau veineux du même doigt enregistré dans la mémoire du terminal de lecture-comparaison ;
- d'autres données nécessaires à l'identification des personnes peuvent être enregistrées dans la mémoire du terminal de lecture-comparaison et associées au gabarit du réseau veineux de leur doigt.

Article 2

Données à caractère personnel traitées

Seules les données à caractère personnel suivantes peuvent être traitées :

- a) Identité : nom, prénom, photographie et gabarit du réseau veineux du doigt de la personne ;
- b) Vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade ;
- c) Déplacement des personnes : porte utilisée, zones et plages horaires d'accès autorisées, date et heure d'entrée et de sortie ;
- d) En cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement.

S'agissant des visiteurs, outre les catégories de données relatives à l'identité et au déplacement des personnes, l'indication de la société d'appartenance et du nom de l'employé accueillant le visiteur peuvent être traitées.

Article 3

Destinataires des informations

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seuls peuvent être destinataires des données limitativement les personnes dûment habilitées :

- du service du personnel et du service informatique : identité, vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking ;
- du service gérant la sécurité des locaux : identité, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking.

Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit du réseau veineux du doigt de la personne que de façon temporaire et pour les stricts besoins de son inscription sur le support individuel ou de sa suppression, sans qu'il leur soit possible d'accéder directement, de modifier, ou de copier sur un autre support, les gabarits enregistrés.

Article 4

Durée de conservation

La durée de conservation du gabarit du réseau veineux des doigts de la main est égale au temps pendant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation.

Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées cinq ans après le départ de l'employé.

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

S'agissant des visiteurs, les catégories de données relatives à l'identité, à l'indication de la société d'appartenance et à la gestion du parking peuvent, au maximum, être conservés trois mois à compter de la date de la dernière visite.

Article 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.

Article 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. Les accès individuels au traitement par l'administrateur du dispositif s'effectuent par un identifiant et un mot de passe individuel ou tout système offrant un niveau de sécurité au moins équivalent. En cas d'utilisation d'un mot de passe, celui-ci doit être régulièrement renouvelé, être d'une longueur d'au moins 8 caractères alphanumériques et comporter au moins un chiffre, une lettre et un caractère de ponctuation.

Le dispositif doit permettre l'enrôlement de plusieurs doigts par utilisateur. Afin d'en garantir la confidentialité, les gabarits enregistrés dans le dispositif doivent être chiffrés en utilisant des algorithmes cryptographiques réputés forts.

Le dispositif doit permettre de détecter toute ouverture ou arrachement du terminal de lecture-comparaison et de le signaler à l'administrateur du système.

Les gabarits traités ne doivent pas permettre de recalculer l'image correspondante du réseau veineux. Au cas où le dispositif comporte un historique des passages, celui-ci ne doit pas conserver des données au-delà de quatre-vingt-dix jours.

Article 7

Information des personnes

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}.

L'information des employés 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.

Article 8

Exercice des droits d'accès et de rectification

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable de traitement aura désignés.

Article 9

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du réseau veineux des doigts de la main 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^o) et 30 de la loi du 6 janvier 1978 modifiée.

Article 10

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

Le président,
A. TÜRK