

Commission nationale de l'informatique et des libertés

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 (décision d'autorisation unique n° AU-27)

NOR : CNIA1100002X

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 ;

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 (I, 8°) ;

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

Vu la loi n° 84-53 du 26 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, modifié par le décret n° 2007-451 du 25 mars 2007, 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 ;

Après avoir entendu M. Emmanuel de Givry, vice-président délégué, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

La gestion du contrôle de l'accès à un poste informatique portable peut s'effectuer grâce à la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales.

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 du traitement mettant en œuvre de tels dispositifs dans le respect des dispositions de cette décision unique adresse à la commission un engagement de conformité de ceux-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.

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

Les postes informatiques portables intégrant des lecteurs d'empreinte digitale sont sous le contrôle exclusif et personnel de l'utilisateur à qui il a été confié. Le fait que l'utilisateur soit en possession du dispositif stockant sa donnée biométrique offre des garanties de confidentialité et de sécurité conformes aux exigences de la loi du 6 janvier 1978 modifiée.

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

– pour le compte de l'Etat ;

- par les établissements accueillant des mineurs, lorsque les personnes concernées par le dispositif sont des mineurs.

Ces traitements peuvent uniquement avoir pour finalité le contrôle de l'accès à des postes informatiques portables professionnels limitativement identifiés de l'organisme, à l'exclusion de tout contrôle du temps de travail de l'utilisateur.

Chaque poste informatique portable intégrant un lecteur d'empreinte digitale doit être sous le contrôle exclusif et personnel de l'utilisateur à qui il a été confié.

Le dispositif de reconnaissance des empreintes digitales doit présenter les caractéristiques suivantes, étant précisé qu'une ou plusieurs empreintes digitales peuvent être utilisées :

- seul le gabarit de l'empreinte digitale, clé biométrique résultat du traitement des mesures par un algorithme, est enregistré sur le poste informatique portable et non une image ou une photographie de l'empreinte digitale ;
- le gabarit de l'empreinte digitale sera stocké chiffré par l'intermédiaire d'un algorithme cryptographique réputé fort ;
- le gabarit traité ne doit pas permettre de recalculer l'image correspondant à l'empreinte ;
- le gabarit de l'empreinte digitale de la personne concernée est exclusivement enregistré sur le poste informatique portable détenu par elle seule et dont le contenu ne peut être lu à son insu ;
- l'enrôlement ne peut être effectué que sur le poste informatique portable de l'utilisateur, si besoin avec l'aide des personnes habilitées du service en charge de la sécurité informatique ;
- le contrôle d'accès s'effectue par une comparaison entre le gabarit de l'empreinte digitale du doigt apposé sur le lecteur et le gabarit de l'empreinte digitale enregistré lors de l'enrôlement de l'utilisateur sur le poste informatique portable ;
- à aucun moment, le gabarit de l'empreinte digitale ne circulera sur un réseau ;
- lors d'opérations de maintenance du poste informatique portable, les données biométriques sont systématiquement effacées, et la procédure d'enrôlement doit être réitérée ;
- afin de parer à un possible problème technique lié au dispositif biométrique, une solution alternative d'authentification telle qu'un identifiant et un mot de passe doit pouvoir être paramétrée sur le poste informatique portable. En cas d'utilisation d'un mot de passe, celui-ci doit être d'une longueur d'au moins 8 caractères alphanumériques et comporter au moins un chiffre, une lettre et un caractère de ponctuation.

Art. 2. – Données à caractère personnel traitées.

Seules les données à caractère personnel suivantes peuvent être traitées :

- identifiant d'utilisateur (tel que le patronyme ou pseudonyme, ou un matricule interne) ;
- mot de passe ;
- gabarit du ou des empreintes digitales.

Art. 3. – Destinataires des informations.

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seules peuvent être destinataires des données, à l'exception du gabarit de l'empreinte digitale, les personnes habilitées du service en charge de la sécurité informatique.

Art. 4. – Durée de conservation.

La durée de conservation du gabarit de l'empreinte digitale est égale au temps pendant lequel la personne concernée est habilitée à accéder à son poste informatique portable dont l'accès est contrôlé.

Les autres données peuvent, au maximum, être conservées cinq ans après le départ de l'utilisateur.

Art. 5. – 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.

L'authentification de l'utilisateur à l'application de gestion du dispositif biométrique s'effectue soit par le dispositif biométrique lui-même, soit par tout autre moyen tel qu'un identifiant et un mot de passe.

Art. 6. – Information des personnes.

Le responsable du traitement procède également, conformément aux dispositions des articles L. 2323-13, L. 2323-14 et L. 2323-32 du code du travail et à la législation applicable aux deux 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 utilisateurs sera 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.

Art. 7. – 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 du traitement aura désignés.

Art. 8. – Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance de l'empreinte digitale enregistrée sur le poste informatique portable de l'utilisateur exclusivement détenu par ce dernier afin d'en contrôler l'accès 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 (I, 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.

Pour le présisent et par délégation :

Le vice-président délégué,

E. DE GIVRY