Commission Nationale de l'Informatique et des Libertés

DELIBERATION n°2015-363 du 15 octobre 2015

Délibération n° 2015-363 du 15 octobre 2015 autorisant Securymind à mettre en œuvre un traitement automatisé de données à caractère personnel reposant sur un dispositif biométrique de reconnaissance combinée du réseau veineux des doigts de la main et de l'empreinte digitale ayant pour finalité le contrôle d'accès aux locaux professionnels.

(Demande d'autorisation n° 1727156)

La Commission nationale de l'informatique et des libertés,

Saisie par la société Securymind d'une demande d'autorisation concernant un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle d'accès aux locaux professionnels par reconnaissance combinée du réseau veineux des doigts de la main et de l'empreinte digitale ;

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 des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 25-I-8°;

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

Vu le dossier et ses compléments ;

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 :

Responsable du traitement	Securymind est un cabinet de conseil en analyse des risques de sûreté des structures sensibles de l'Etat français et d'entreprises soumises à des obligations de sûreté, ayant le statut de société à responsabilité limitée. Il doit dans ce cadre garantir à ses clients la disponibilité, l'intégrité et la confidentialité des informations sensibles qui lui sont confiées ainsi que la sécurité des matériels soumis à autorisation gouvernementale nécessaires pour exécuter ses missions. Plusieurs accréditations lui ont été accordées à ce titre. Le cabinet doit justifier d'un niveau de sécurité élevé pour l'accès à ses locaux.
Sur la finalité et les caractéristiques du traitement	Le dispositif biométrique bimodal, fondé sur la reconnaissance de l'empreinte digitale et du réseau veineux d'un doigt de chaque main, est mis en place afin de lutter contre le risque d'usurpation d'identité lors de l'accès aux locaux du cabinet. Le dispositif est composé d'un seul et même lecteur qui permet de lire le réseau veineux et l'empreinte digitale d'un doigt d'une personne de manière simultanée. La reconnaissance biométrique

	utilisée est fondée sur la comparaison d'informations issues de l'empreinte digitale et du réseau veineux d'un individu avec un gabarit unique. Le gabarit est stocké sur le terminal selon un format propriétaire. Le terminal est isolé des autres traitements et sans connexion à internet ou au réseau. Le recours à la biométrie multimodale améliore les performances globales des dispositifs biométriques en offrant plus de critères de contrôle, en renforçant ainsi le niveau d'authentification et en compensant les faiblesses, avérées ou supposées, d'une biométrie par une autre. De plus la solution utilisée permet de limiter les risques sur les individus créés par le système à un niveau équivalent à une biométrie « sans trace ». Le renforcement du contrôle d'accès au moyen d'un dispositif biométrique répond aux besoins particuliers du cabinet Sécurymind, notamment en termes de sécurité des données traitées dans le cadre de son activité d'analyse et de conseil en matière de risques de sûreté des structures sensibles de l'Etat français et d'entreprises soumises à des obligations de sûreté. La Commission considère que la finalité ainsi définie est déterminée, explicite et légitime.
Sur les données traitées	Les données concernent les salariés habilités. Il s'agit : · des données d'identification : nom et prénom des personnes concernées ; · de l'historique d'accès aux locaux : horodatage des accès et identifiant du lecteur ; · des données biométriques de l'empreinte digitale et du réseau veineux de deux doigts. · La Commission considère que ces données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.
Sur la durée de conservation des données	Les données relatives à l'historique d'accès et les données d'identification sont conservées sur une période de trois mois glissants dans le serveur de Securymind. Les données biométriques ne sont conservées que le temps de l'habilitation d'accès de la personne concernée, sur le terminal de lecture comparaison. En cas de départ de cette dernière, le gabarit biométrique est immédiatement supprimé, sous le contrôle de l'officier de sûreté du cabinet.
Sur les destinataires	Seul le personnel spécifiquement habilité de Securymind peut accéder aux données d'identification ainsi qu'à l'historique d'accès, ce qui n'appelle pas d'observation de la Commission.
Sur l'information et le droit d'accès	Le dispositif a fait l'objet d'une consultation des instances représentatives du personnel.

	Les personnes concernées sont informées de manière individuelle, par un message électronique d'information spécifique et détaillé et lors d'une réunion d'information. Les droits s'exercent auprès des services du responsable de traitement. La Commission estime que ces modalités d'information et d'exercice des droits sont satisfaisantes.
Sur les mesures de sécurité	La Commission relève que le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles ne soient déformées ou endommagées ou que des tiers non autorisés y aient accès. Une formation est dispensée par l'intégrateur à toutes les personnes habilitées. En cas de faille de sécurité, le personnel de sécurité présent sur site est formé pour réagir rapidement selon la situation. En cas de défaillance du dispositif, des entrées de secours contrôlées par 3 personnes du cabinet peuvent être utilisées. Compte tenu de l'objectif de sécurité recherché, des exigences fortes de fiabilité du système et de sécurité des données traitées ont été définies. A titre principal, il s'agit : · du choix spécifique du dispositif biométrique limitant les risques de fausse acceptation (personne faussement reconnue et autorisée à accéder de manière illégitime) ; · du chiffrement du gabarit (format propriétaire) avec une clé spécifique au traitement ; · du signalement de toute tentative d'accès aux lecteurs (dispositif anti-arrachement) ; · du signalement de toute tentative d'accès par une personne dont le gabarit d'empreinte ne se trouve pas dans le lecteur ; · du nombre limité de personnes habilitées à la gestion (enrôlement, administration) du dispositif. · le gabarit fusionné ne peut pas permettre de créer un gabarit utilisable pour une seule des deux biométries ; · le gabarit ne permet pas de recalculer l'image correspondante du réseau veineux ou de l'empreinte digitale. Enfin, la Commission souligne que le dispositif utilisé apporte les deux garanties suivantes : · du choix spécifique du dispositif biométrique limitant les risques de fausse acceptation (personne faussement reconnue et autorisée à accéder de manière illégitime) ; · du chiffrement du gabarit (format propriétaire) avec une clé spécifique au traitement ;

	· du signalement de toute tentative d'accès aux lecteurs (dispositif anti-arrachement) ; · du signalement de toute tentative d'accès par une personne dont le gabarit d'empreinte ne se trouve pas dans le lecteur ; · du nombre limité de personnes habilitées à la gestion (enrôlement, administration) du dispositif. · le gabarit fusionné ne peut pas permettre de créer un gabarit utilisable pour une seule des deux biométries ; · le gabarit ne permet pas de recalculer l'image correspondante du réseau veineux ou de l'empreinte digitale. · Les mesures de sécurité mises en place sont conformes à l'exigence de sécurité prévue par l'article 34 de la loi du 6 janvier 1978 modifiée. La Commission rappelle toutefois que cette obligation nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Autorise, conformément à la présente délibération, la société Securymind à mettre en œuvre le traitement susmentionné.

La Présidente
I. FALQUE-PIERROTIN