

JOAQUIN BAYO DELGADO
CONTROLEUR ADJOINT

M. Philippe RENAUDIÈRE
Délégué à la protection des données
Commission européenne
BRU BERL 08/180
B - 1049 BRUXELLES

Bruxelles, le 9 juin 2009
JBD/DH/ktl D(2008)1837 C 2008-721

Objet: Système de gestion de l'accès au CCR-IE de Petten

Monsieur,

Je me réfère à la notification en vue d'un contrôle préalable relatif au traitement des données à caractère personnel concernant le "Système de gestion de l'accès au CCR-IE de Petten" transmise par le Centre commun de recherche (2008-721).

L'article 27, paragraphe 1, du règlement soumet au contrôle préalable du CEPD les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités. L'article 27, paragraphe 2, du règlement énumère les traitements susceptibles de présenter des risques particuliers au sens susvisé.

Notification

Dans la notification adressée au CEPD, le contrôle d'accès à l'IE (Petten) est présenté comme un ensemble de sous-processus dont la finalité principale est de restreindre l'accès des personnes non autorisées aux installations et aux zones sensibles de l'IE pour des raisons de sécurité et de sûreté. Il était souligné dans la notification que le traitement relevait de l'article 27, paragraphe 2, point a): traitement de données relatives à des mesures de sûreté.

Analyse du CEPD concernant le traitement

Étant donné que ce n'est pas la première fois qu'un traitement similaire concernant le contrôle d'accès est notifié par le CCR¹, le CEPD souhaiterait attirer l'attention sur les aspects suivants:

L'article 27, paragraphe 2, point a), dispose que les traitements de données "*relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté*" sont soumis au contrôle préalable du CEPD.

Contrairement à ce qui est décrit dans la notification, le CEPD interprète de manière constante la notion de "mesures de sûreté" visée à l'article 27, paragraphe 2, point a), non pas comme désignant des mesures ayant trait à la protection physique et à la sécurité des bâtiments et du personnel, mais plutôt comme désignant des mesures prises à l'égard de personnes dans le contexte d'une procédure pénale (ou administrative) ('mesures de sûreté'). En effet, les mesures de sûreté concernent les "suspicions, infractions, condamnations pénales" citées dans le même article.

Il convient d'interpréter les "mesures de sûreté" décrites à l'article 10 du règlement 45/2001 de la même manière. Les mesures de sûreté concernent les "infractions, condamnations pénales" citées dans le même article et désignent les mesures prises à l'égard de personnes dans le contexte d'une procédure pénale (ou administrative).

Le CEPD considère que les traitements concernant la "gestion du contrôle d'accès" ne sont soumis au contrôle préalable que s'ils présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités en vertu de l'article 27, paragraphe 1. C'est par exemple le cas lorsque les traitements font appel à des systèmes de traitement biométrique pour gérer le contrôle d'accès. L'opinion du CEPD se fonde principalement sur la nature des données biométriques, qui sont extrêmement sensibles en raison de certaines des caractéristiques qui leur sont inhérentes. Ainsi, les données biométriques modifient irrévocablement la relation entre le corps et l'identité en ce sens qu'elles rendent les caractéristiques du corps humain "lisibles par une machine" et susceptibles d'être utilisées ultérieurement. Outre la nature extrêmement sensible de ces données, le CEPD relève également les possibilités d'interconnexions et l'état actuel des outils technologiques, qui peuvent avoir des conséquences inattendues ou fâcheuses pour les personnes concernées.

Par conséquent, si le CCR-IE envisage de recourir à des systèmes de traitement biométrique dans le cadre du traitement en vue de la gestion de l'accès, il devra adresser une nouvelle notification au CEPD en temps utile et tous les aspects techniques du traitement ayant trait au recours à la biométrie devront être clairement expliqués dans la notification pour contrôle préalable. Comme l'indique l'expression "contrôle préalable", le contrôle du CEPD devrait intervenir avant le début du traitement.

Enfin, le CEPD souhaiterait insister sur le fait que, indépendamment de la nécessité ou non d'un contrôle préalable, le traitement doit respecter le règlement n° 45/2001. Cela signifie par exemple que la durée de conservation doit être modifiée afin de respecter l'article 4, paragraphe 1, point e): "*les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées (...)*". Dans des cas similaires, le CEPD a considéré que la durée de conservation nécessaire était de trois mois au maximum.

¹ "Contrôle d'accès au CCR-IPTS de Séville", dossier 2007-375, publié le 17 juillet 2007, "Contrôle d'accès à l'IRMM de Geel", dossier 2007-376, publié le 16 juillet 2007, cf. site Internet du CEPD: <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/72#2007>

Conclusion

Après avoir soigneusement analysé les informations disponibles, le CEPD conclut que le traitement dont il est question ici et qui est décrit dans la notification n'est pas soumis au contrôle préalable au titre de l'article 27 du règlement (CE) n° 45/2001.

Le CEPD vous saurait gré de bien vouloir communiquer ces considérations au contrôleur et de nous informer de la suite qui sera donnée à la recommandation sur la conservation des données dans un délai de trois mois à compter de la réception de la présente lettre.

Nous restons bien évidemment à votre disposition pour toute nouvelle consultation sur cette question.

(Formule de politesse)

(signé)

Joaquín BAYO DELGADO
