Coopération transfrontière pour lutter contre le terrorisme et la criminalité transfrontière, mise en œuvre du traité de Prüm. Initiative Allemagne

2007/0821(CNS) - 19/12/2007 - Document annexé à la procédure

AVIS DU CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES surl'initiative de l'Allemagne en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/…/JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière.

Le CEPD n'a pas été invité à formuler un avis sur l'initiative. Il rend donc son avis d'office comme il l'a fait à d'autres occasions.

Conclusions du CEPD : le CEPD recommande que l'initiative et son annexe fassent l'objet d'un débat ouvert auquel contribueraient tous les acteurs institutionnels, compte tenu également du rôle de co-législateur à part entière que jouera le Parlement européen dans ce domaine lorsque le traité de Lisbonne entrera en vigueur. Il invite le législateur à veiller à ce qu'**un cadre juridique clair, efficace et complet en matière de protection des données**, combinant différents instruments juridiques et des dispositions générales et des garanties spécifiques, soit en place avant l'entrée en vigueur de l'initiative.

Dans cette optique, le CEPD réaffirme :

- que les décisions du Conseil concernant le traité de Prüm ne devraient pas entrer en vigueur avant que les États membres aient mis en œuvre une décision-cadre générale sur la protection des données dans le cadre du 3ème pilier, qui serait une «*lex generalis*» complétée par les dispositions de l'initiative de Prüm permettant l'application de garanties spécifiques et de normes plus strictes spécialement définies ;
- le législateur devrait préciser que les règles spécifiques en matière de protection des données concernant **l'ADN, les empreintes digitales et l'immatriculation des véhicules** prévues au chapitre 6 de l'initiative de Prüm, seront applicables non seulement à l'échange de ces données, mais aussi à leur collecte, à leur conservation et à leur traitement au niveau national, ainsi qu'à la fourniture d'autres données à caractère personnel relevant du champ d'application de la décision du Conseil.

Globalement, le CEPD recommande d'améliorer la transparence des mesures envisagées avec la mise à disposition, le plus rapidement possible, de la version définitive de l'annexe et la mise en place de mécanismes d'information des citoyens sur les caractéristiques des systèmes, sur leurs droits et sur les moyens de les exercer. Il invite le législateur à prendre dûment en considération la taille du système en veillant à ce que l'augmentation du nombre d'États membres participants n'implique pas une diminution de l'efficacité de ce système.

Le CEPD recommande par ailleurs que le **rôle consultatif** essentiel des autorités compétentes en matière de protection des données soit explicitement reconnu. L'initiative devrait notamment garantir que les États membres fournissent aux autorités chargées de la protection des données, les ressources (complémentaires) nécessaires pour mener à bien leur rôle de supervision.

Le CEPD invite donc une nouvelle fois le législateur à introduire une **définition claire et complète des données à caractère personnel**. Dans cette optique, les dispositions de mise en œuvre devraient

également clarifier l'applicabilité des règles de protection des données aux profils d'ADN non identifiés. Le CEPD rappelle aussi que la définition de la «partie non codante» de l'ADN devrait pouvoir évoluer.

Le CEPD recommande encore que, dans le contexte des consultations et des comparaisons automatisées, l'exactitude du **processus d'établissement de la concordance** soit dûment prise en compte (ex. : pour les empreintes digitales ou les profils ADN, l'initiative devrait harmoniser le plus possible les différents systèmes utilisés dans les États membres et la manière dont ces systèmes sont utilisés).

Il demande enfin que l'on mette l'accent sur **l'évaluation des aspects relatifs à la protection des données dans le cadre des échanges d'informations**, en accordant une attention particulière à la finalité de ces échanges, aux méthodes d'information des personnes concernées, à l'exactitude des données échangées et aux fausses concordances, aux demandes d'accès aux données à caractère personnel, à la durée de conservation des données et à l'efficacité des mesures de sécurité. Dans ce contexte, la participation des autorités et des experts compétents en matière de protection des données devrait être prévue.