Agence de l'Union européenne pour la coopération des services répressifs (Europol)

2013/0091(COD) - 31/05/2013 - Document annexé à la procédure

Avis du Contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI.

Le 27 mars 2013, la Commission a adopté la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI. Le même jour, la Commission a transmis cette proposition pour consultation au CEPD.

L'avis du CEPD est axé sur les modifications les plus significatives du cadre juridique d'Europol du point de vue de la protection des données.

Protections des données dans le cadre des institutions européennes: le CEPD recommande de préciser dans les considérants de la proposition que le nouveau cadre de la protection des données des institutions et des organes de l'Union européenne s'appliquera à Europol dès son adoption. Au plus tard dès l' adoption du nouveau cadre général, les principaux nouveaux éléments de la réforme de la protection des données (à savoir le principe de responsabilité, l'analyse d'impact relative à la protection des données, la prise en compte du respect de la vie privée dès la conception et la protection de la vie privée par défaut ainsi que la notification de violations de données à caractère personnel) devraient aussi s'appliquer à Europol.

Transferts de données à des tiers: le CEPD propose une série de dispositions nouvelles sur la question du transfert de données. Tout en saluant le fait que le transfert de données vers des pays tiers et des organisations internationales ne pourrait avoir lieu que s'il est adéquat ou si un accord contraignant fournit des garanties appropriées, le CEPD demande qu'un **accord contraignant** garantisse la sécurité juridique ainsi que la responsabilité d'Europol en ce qui concerne le transfert (surtout pour les transferts massifs, structurels et fréquents de données). Le CEPD comprend cependant qu'il existe des situations dans lesquelles un accord contraignant ne peut être requis. Ces situations devraient être exceptionnelles et fondées sur une réelle nécessité, uniquement **dans des cas limités**. Elles devraient également être fondées sur des garanties solides, aussi bien au niveau du fond qu'au niveau de la procédure.

Le CEPD recommande par ailleurs de **supprimer la possibilité pour Europol de supposer l' autorisation des États membres**. Il conseille également d'ajouter que l'autorisation devrait être accordée «avant le transfert». Il recommande en outre d'ajouter à la proposition une disposition transitoire relative aux accords de coopération existants et régissant les transferts de données à caractère personnel par Europol.

Le CEPD recommande par ailleurs :

- d'ajouter expressément que les dérogations ne pourraient s'appliquer aux transferts fréquents, massifs ou structurels par opposition aux transferts occasionnels;
- de prévoir un paragraphe spécifique consacré aux transferts effectués avec l'autorisation du CEPD. Cette autorisation devrait être accordée avant le transfert/l'ensemble de transferts, pour une période ne dépassant pas un an, renouvelable.

Autres recommandations: le CEPD recommande par ailleurs de:

- supprimer la possibilité pour Europol d'accéder directement aux bases de données nationales;
- lorsque l'accès concerne des systèmes d'information européens, n'accorder l'accès que sur la base du système de «hit/no hit» (à savoir une réponse positive ou négative). Toute information relative au «hit» devrait être communiquée à Europol après l'approbation et l'autorisation explicites du transfert par l'État membre;
- inclure dans la proposition, une disposition selon laquelle Europol devrait adopter une politique transparente et facilement accessible expliquant son traitement des données à caractère personnel et aux fins de l'exercice des droits des personnes concernées. Cette politique devrait prendre une forme intelligible et utiliser un langage clair et simple;
- ajouter des dispositions relatives au maintien des principes de protection des données dès la conception des systèmes de traitement des données à caractère personnel.