

Politique antiterroriste de l'UE: le CEPD appelle à une approche systématique et cohérente pour éviter des restrictions inutiles à la vie privée

Le Contrôleur européen de la protection des données (CEPD) a publié aujourd'hui un avis sur la communication de la Commission européenne sur la politique antiterroriste de l'UE qui présente les principales réalisations et les défis futurs, et prépare la voie à une stratégie plus large sur la sécurité intérieure^(*). La communication fait partie d'un certain nombre de documents dans lesquels la Commission expose les politiques qu'elle entend mener dans ce domaine. La Commission a par exemple publié lundi une autre communication portant sur "La stratégie de sécurité intérieure de l'UE en action".

Le CEPD insiste sur la nécessité d'assurer une cohérence et d'établir clairement les relations entre les différentes politiques et initiatives adoptées dans le domaine des affaires intérieures et de la sécurité intérieure. La communication présente des liens étroits avec d'autres initiatives existantes, tels que les mesures restrictives et le gel des avoirs, la conservation des données, la biométrie, les données relatives aux passagers aériens et l'accord TFTP/SWIFT sur l'échange de données financières. Le CEPD souligne que bon nombre de ces mesures ont été prises rapidement en réponse à des incidents terroristes, sans examen approfondi des chevauchements éventuels avec les instruments existants.

Le CEPD se félicite de l'attention accordée aux droits fondamentaux et à la protection des données dans la communication. Il partage le point de vue de la Commission selon lequel une approche systématique dans le domaine doit être préférée à une prise de décision réactive axée sur les incidents, en particulier lorsque ces derniers conduisent à la création de nouveaux systèmes de stockage, de collecte et d'échange de données, sans avoir procédé à une évaluation appropriée des solutions existantes.

Selon Peter Hustinx, CEPD: "*Le droit à la protection des données personnelles est un allié nécessaire pour promouvoir la sécurité juridique, la confiance et la coopération dans la lutte contre le terrorisme. C'est aussi une condition juridique indispensable pour le développement de nouveaux systèmes de collecte de données. Des restrictions inutiles à la vie privée des citoyens doivent être évitées lorsque de nouvelles mesures sont envisagées. Il convient pour cela d'évaluer les éventuels chevauchements avec les instruments existants et de limiter la collecte et l'échange de données personnelles à ce qui est vraiment nécessaire pour atteindre les objectifs poursuivis.*"

Le CEPD recommande également des améliorations concrètes dans des domaines tels que:

- **les mesures relatives au gel des avoirs:** une approche complète et globale sur le recours à des mesures restrictives à l'égard de pays spécifiques et des terroristes présumés devrait être proposée afin d'assurer l'efficacité de l'action répressive et le respect des droits fondamentaux;
- **la coopération internationale:** le CEPD souligne la nécessité d'assurer des garanties adéquates lorsque les données personnelles sont traitées dans le cadre de la coopération internationale, tout en favorisant le développement et la mise en œuvre des principes de protection des données par les pays tiers et les organisations internationales;
- **"privacy by design":** le législateur européen devrait s'assurer que l'expertise en matière de protection des données est introduite à un stade précoce dans la recherche sur la sécurité, de manière à guider les options politiques et à garantir que la vie privée est pleinement intégrée dans les nouvelles technologies axées sur la sécurité.

Dans une perspective plus large, le CEPD invite la Commission à présenter une proposition visant à la mise en place d'un cadre de protection des données dans le domaine de la politique étrangère et de sécurité commune.

(*) Communication du 20 juillet 2010 de la Commission au Parlement européen et au Conseil: "La politique antiterroriste de l'UE: principales réalisations et défis à venir" (COM(2010)386 final)