

Lutte contre le terrorisme: traitement et protection des données personnelles dans le cadre de la coopération policière et judiciaire en matière pénale. Décision-cadre

2005/0202(CNS) - 25/01/2012 - Document de suivi

La Commission présente un rapport sur l'état de la mise en œuvre de la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Les principaux points de ce rapport peuvent se résumer comme suit :

Champ d'application des mesures nationales de mise en œuvre : la décision-cadre s'applique au seul traitement des données à caractère personnel transmises ou mises à disposition entre les États membres (article 1^{er}, paragraphe 2). Le traitement des données à caractère personnel par la police et la justice dans le cadre d'affaires pénales au niveau national ne relève pas de cette décision-cadre. **Trois États membres ont considéré que le champ d'application limité de la décision-cadre constituait un problème.** L'Italie et les Pays-Bas ont évoqué la difficulté d'établir, dans la pratique, une distinction entre le traitement transfrontière des données conformément à la décision-cadre 2008/977 et le traitement de celles-ci au niveau national, ainsi que la difficulté en découlant pour les autorités répressives nationales de s'adapter à des règles de traitement différentes applicables aux mêmes données à caractère personnel. De manière générale, la Pologne a relevé les lacunes de la décision-cadre et a, notamment, exprimé son soutien à l'objectif poursuivi par la Commission d'instituer un cadre global et d'étendre les règles générales en matière de protection des données au domaine de la coopération policière et judiciaire en matière pénale.

Information des personnes concernées par les données (article 16) : conformément à la décision-cadre, les États membres doivent veiller à ce que les autorités nationales compétentes informent les personnes concernées que leurs données sont traitées ou ont été transmises à un autre État membre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales. Presque tous les États membres ont déclaré fournir aux personnes concernées certaines informations relatives au traitement de leurs données à caractère personnel. La France a indiqué qu'elle ne le faisait pas. Le Danemark n'accorde pas non plus ce droit, mais a signalé que le responsable du traitement doit tenir un registre et informer le public. Le droit d'information fait l'objet de limitations dans la grande majorité des États membres. Les Pays-Bas ont déclaré que l'obligation générale d'informer la personne concernée par les données n'était pas totalement compatible avec la nature du travail de la police et de la justice, mais que certaines dispositions avaient été prises pour répondre suffisamment à l'obligation d'informer la personne concernée au sujet du traitement de données par les autorités policières et judiciaires. La décision-cadre institue également le droit à l'information des personnes concernées par les données mais ne comporte aucune précision quant à la méthode à employer ou à d'éventuelles exceptions en la matière. Même si, aux dires des États membres, le droit à l'information est généralement accordé, sa mise en œuvre varie considérablement.

Droit d'accès des personnes concernées par les données (article 17) : la décision-cadre contient des dispositions générales conférant aux personnes concernées le droit de consulter leurs données. Elle ne détaille pas le type d'informations à fournir aux personnes concernées. Elle laisse également aux États membres le soin de décider si ces personnes peuvent exercer ce droit d'accès directement ou si elles doivent le faire par la voie indirecte. Tous les États membres accordent, dans une certaine mesure, un droit

d'accès aux personnes concernées par les données. Ce droit est généralement inscrit dans la législation nationale générale en matière de protection des données. De nombreux États membres réglementent également les modalités du droit d'accès dans la législation sectorielle (comme la législation policière). De même, les États membres prévoient tous des dérogations au droit d'accès. Les motifs les plus fréquemment invoqués pour refuser le droit d'accès sont la prévention, la recherche, la détection et la poursuite d'infractions pénales et la sûreté de l'État, la défense et la sécurité publique.

Autres questions soulevées par les États membres : 6 États membres ont formulé des commentaires sur des sujets qui les préoccupent :

- la Pologne a considéré que la décision-cadre présentait de nombreuses lacunes auxquelles il convenait de remédier et s'est déclarée favorable à une réforme en vue de l'instauration d'un régime global et cohérent de protection des données au niveau de l'Union;
- l'Italie et les Pays-Bas ont évoqué la difficulté d'établir dans la pratique une distinction entre le traitement transfrontière des données conformément à la décision-cadre 2008/977 et le traitement de celles-ci au niveau national, ainsi que la difficulté en découlant pour les services répressifs nationaux de s'adapter à des règles de traitement différentes applicables aux mêmes données à caractère personnel;
- l'Italie, la République tchèque et les Pays-Bas ont désapprouvé les règles relatives aux transferts internationaux prévues dans la décision-cadre. En particulier, l'Italie a déclaré qu'il était nécessaire de prévoir un niveau adéquat et plus uniforme de protection pour les transferts de données vers des pays tiers. Les Pays-Bas ont considéré comme problématique que la décision-cadre ne fixe pas de critères permettant de déterminer le caractère adéquat de la protection assurée par un pays tiers, ce qui donne lieu à une mise en œuvre hétérogène de celle-ci par les États membres. Quant à la République tchèque, elle a jugé «irréaliste» de prévoir dans la décision-cadre des règles relatives aux transferts internationaux;
- la France a évoqué un problème qui lui est propre en ce qui concerne les durées de conservation des données à caractère personnel transférées à un pays tiers ou reçues d'un tel pays dont les exigences à cet égard sont différentes;
- la Slovaquie a souligné la nécessité d'établir une distinction plus marquée entre le traitement de données par la police et par le pouvoir judiciaire (procédures juridictionnelles);
- la République tchèque et les Pays-Bas ont tous deux indiqué qu'il était déroutant pour les autorités répressives de devoir se conformer à de multiples règles relatives à la protection des données existant aux niveaux international (telles celles édictées par le Conseil de l'Europe), européen et national.

Le rapport estime que les difficultés pratiques rencontrées par un certain nombre d'États membres pour établir la distinction entre règles applicables respectivement au traitement national de données et traitement transfrontière de celles-ci pourraient être résolues grâce à **un corps unique de règles visant le traitement de données tant au niveau national que dans un contexte transfrontière**. Il conviendrait de clarifier davantage, au niveau de l'Union, le champ d'application du droit d'information des personnes concernées par les données ainsi que les éventuelles dérogations à ce droit. La **définition de critères harmonisés minimaux** en ce qui concerne le droit d'accès des personnes concernées par les données pourrait renforcer les droits de ces personnes tout en prévoyant des dérogations pour permettre aux services de police et de justice de remplir convenablement leurs missions.

En vertu de l'article 16 du traité sur le fonctionnement de l'Union européenne, qui consacre le droit à la protection des données à caractère personnel, il est possible à présent d'instituer un cadre global relatif à la protection des données garantissant à la fois un niveau élevé de protection des données des personnes physiques dans le domaine de la coopération policière et judiciaire en matière pénale, et des échanges plus fluides des données à caractère personnel entre les autorités nationales policières et judiciaires, dans le respect entier du principe de subsidiarité.