Système d'information Schengen de deuxième génération (SIS II): établissement, fonctionnement et utilisation

2005/0103(CNS) - 25/10/2006 - Texte adopté du Parlement, 1ère lecture/lecture unique

En adoptant par 521 voix pour, 72 contre et 65 abstentions, le rapport de M. Carlos **COELHO** (PPE-DE, PT), le Parlement a avalisé en Plénière le compromis obtenu avec le Conseil sur le dossier du SIS II, en vue d'aboutir à un accord en 1ère lecture.

Ce faisant, le Parlement propose une **version consolidée** du compromis obtenu avec le Conseil, et ce, pour les 3 propositions qui faisaient l'objet du paquet «SIS II» (incluant à la fois la présente proposition mais aussi le règlement parallèle : **COD/2005/0106**). La base juridique globale du SIS intègre en effet 2 instruments complémentaires mais séparés qui constituent ensemble (règlement + décision) le fondement juridique complet du SIS, le 3ème instrument étant plus technique (voir **COD/2005/0104**) et venant compléter le cadre juridique général destiné à prendre le relais du SIS1+ existant et à accueillir dès que possible les nouveaux États membres.

Si globalement, le Parlement européen approuve l'approche de la Commission, il introduit de très nombreux amendements destinés à **améliorer les normes de protection et de sécurité des données à caractère personnel** du système. La plupart des amendements de compromis adoptés en Plénière avaient été négociés le 26 septembre 2006 lors d'un trilogue informel avec la Commission et le Conseil.

Toutefois, la Plénière a refusé d'introduire un changement demandé par l'Allemagne qui permettrait aux services de renseignements nationaux d'avoir accès aux informations stockées dans SIS II (à noter que le refus de répondre à la demande de la délégation allemande risque de ralentir l'adoption du dossier tout entier en 1ère lecture car si l'Allemagne campe sur cette position, le paquet SIS II pourrait alors faire l'objet d'une 2ème lecture au PE et faire obstacle à la demande du Conseil d'aboutir à un accord rapide en vue de pouvoir faire démarrer le système début 2007).

Principales caractéristiques du compromis :

1) **création d'une « Autorité de gestion »:** le Parlement, en accord avec le Conseil, demande la création d'une autorité de gestion, financée par le budget communautaire, qui gérera le fonctionnement de la base de données centrale du SIS II. Dans un 1er temps, la Commission serait chargée de la gestion opérationnelle du SIS II central et de l'infrastructure de communication. Afin d'assurer une transition en douceur entre le SIS1+ et le SIS II, elle pourrait déléguer les responsabilités à des organismes publics nationaux, avant la mise en place de l'instance gestionnaire finale permanente. La période transitoire ne pourrait excéder 5 ans à compter de l' entrée en vigueur du SIS II. L'instance gestionnaire devrait présenter un rapport sur le fonctionnement du SIS tous les 2 ans, y compris sur le niveau de sécurité qu'il offre et sur les échanges d'informations supplémentaires ; la Commission réaliserait une évaluation globale du système tous les 4 ans ;

2) **signalements** : le SIS devrait contenir des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition. Outre ces signalements, d'autres échanges « *supplémentaires* » seraient prévus destinés à faciliter la remise ou l'extradition de personnes (notamment, les informations destinées à lancer un mandat d'arrêt européen). Le SIS II

comporterait également des données sur les personnes disparues, recherchées dans le cadre d'une procédure judiciaire, les objets ou personnes faisant l'objet de surveillance discrète ou les objets destinés à être saisis ou permettant de servir de preuve dans le cadre d'une procédure pénale. Si un « indicateur de validité » (voir proposition initiale) est apposé sur un signalement concernant une personne à arrêter ou à être remise et que cette personne est dûment localisée dans un État membre, ce lieu pourra être communiqué à qui de droit en vue de faciliter la procédure de mandat d'arrêt européen ;

3) **utilisation de la biométrie** : pour renforcer la fiabilité et augmenter les capacités du système, des données biométriques seraient introduites dans le SIS (photographies et empreintes digitales) mais qui ne pourraient être introduites qu'après un **contrôle de qualité spécial** pour s'assurer du respect d'une norme de qualité minimale des données. Toute recherche sur une base biométrique serait ainsi exclue au stade initial de la mise en place du système et mais serait possible quand ce dernier serait techniquement viable (ceci afin d'éviter toute erreur néfaste sur une personne signalée). Le Parlement européen devra en outre être consulté par la Commission européenne avant la mise en œuvre de cette recherche biométrique ;

4) **interconnexion et compatibilité des signalements** : le compromis prévoit qu'il soit possible de connecter le signalement d'un objet volé avec celui d'une personne recherchée en vue d'une arrestation. Il faudra toutefois pour cela qu'un État membre crée une connexion entre les signalements mais uniquement en cas de besoin opérationnel clair ; le dispositif prévoit le transfert des données du SIS 1+ au SIS II dans le cadre d'une compatibilité renforcée des données de l'un vers l'autre système et moyennant la mise en place d'une période transitoire au cours de laquelle la compatibilité des signalements serait dûment examinée. Dans ce contexte, la compatibilité des signalements de personnes devra faire l'objet **d'une priorité absolue**, et toute modification, ajout, correction ou mise à jour d'un signalement transféré du SIS 1+ au SIS II ainsi que toute réponse positive à un tel signalement devra déclencher un examen immédiat pour vérifier sa conformité avec les dispositions du règlement (notamment, en termes de protection des données) ;

5) **règles techniques d'introduction des données** : de par leur nature hautement technique et leur niveau de précision, des règles techniques très précises devraient être élaborées sur l'introduction des données, l'introduction des signalements, les mises à jour, les suppressions et de consultation …qui ne peuvent être couvertes par le présent dispositif. Les compétences d'exécution en la matière seraient déléguées à la Commission. Une analyse d'impact ultérieure pourrait déterminer si, à l'avenir, l'instance gestionnaire pourrait assumer la responsabilité des mesures d'application y afférentes ;

6) **délai de conservation des données** : les données ne devraient pas être conservées dans le SIS II pour une durée excédant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été fournis et en tout état de cause, les signalements de personnes devraient **automatiquement disparaître au bout de 3 ans** et les signalement d'objets au bout de **5 ans**. Les objets introduits pour saisie ou preuve dans le cadre d'une procédure pénale pourraient toutefois être conservés pendant **10 ans**. La décision de conserver les données relatives aux personnes devrait se fonder sur une évaluation individuelle complète ;

7) **transfert de données à des tiers** : les données traitées dans le SIS ne devraient pas être transférées à un pays tiers ou une organisation internationale. Toutefois, il serait possible de renforcer la coopération entre l'UE et Interpol à condition de garantir que l'échange de données à caractère personnel bénéficie d'un niveau de protection adéquat, garanti par un accord ;

8) **protection des données échangées** : la surveillance des activités de traitement des données personnelles serait du ressort du Contrôleur européen de la protection des données (CEPD) pour ce qui concerne les activités des institutions et organes communautaires. Ces activités feraient l'objet

d'un audit de haut niveau au moins tous les 4 ans. Le traitement des données au niveau national ferait aussi l'objet d'audits confiés aux autorités nationales de supervision en coopération avec le CEPD afin d'assurer la coordination de la supervision. Chaque État membre aurait la responsabilité d'établir et de maintenir un système national de données susceptible de communiquer avec SIS II central et devrait désigner une autorité dans ce but. Il devra notamment prendre les mesures nécessaires pour protéger et échanger les données à caractère personnel en toute licéité.

Á noter encore, des dispositions nouvelles sur :

- la confidentialité des données relatives aux fonctionnaires des Communautés ;

- la mise en place d'un plan de sécurité de la Commission et des États membres visant à faciliter une mise en œuvre effective des obligations en matière de sécurité et en vue de coopérer sur les questions de sécurité dans une perspective commune ;

- la coopération technique à envisager avec les représentants islandais, norvégiens et suisses dans le cadre de la mise en œuvre du SIS II, sachant qu'ils sont directement associés à sa mise en place ;

- la fixation, à terme, d'échéances déterminées pour la participation du Royaume-Uni, de l'Irlande, de la Suisse et des nouveaux États membres au SIS II.