Système d'information Schengen (SIS) dans le domaine des contrôles aux frontières

2016/0408(COD) - 10/11/2017 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des libertés civiles, de la justice et des affaires intérieures a adopté le rapport de Carlos COELHO (PPE, PT) sur la proposition de règlement du Parlement européen et du Conseil sur létablissement, le fonctionnement et lutilisation du système dinformation Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant le règlement (UE) n° 515/2014 et abrogeant le règlement (CE) n° 1987/2006.

La commission parlementaire a recommandé que la position du Parlement européen adoptée en première lecture suivant la procédure législative ordinaire modifie la proposition de la Commission comme suit.

Architecture du système: la proposition de la Commission oblige tous les États membres à disposer dune copie nationale comprenant une copie complète ou partielle de la base de données du SIS ainsi quun N.SIS de secours. Compte tenu du risque pour la sécurité des données, les députés estiment que les États membres ne devraient pas être tenus de posséder une copie nationale aux fins de garantir la disponibilité du système.

Comme moyen supplémentaire de garantir la disponibilité ininterrompue du SIS, les députés ont proposé quune infrastructure de communication de secours soit mise au point et soit utilisée en cas de défaillance de linfrastructure de communication principale.

En particulier, le «CS-CIS» (contenant la base de données du SIS) ou sa version de secours devraient contenir une copie supplémentaire de la base de données du SIS et être utilisés simultanément en fonctionnement actif. Le CS-SIS et sa version de secours devraient être installés sur les sites techniques de lAgence européenne pour la gestion opérationnelle des systèmes dinformation à grande échelle au sein de lespace de liberté, de sécurité et de justice (l«agence eu-LISA»).

Responsabilités incombant aux États membres: chaque État membre devrait désigner une autorité nationale opérationnelle 24 heures sur 24 et 7 jours sur 7 chargée dassurer léchange et la disponibilité de toutes les informations supplémentaires (le «bureau SIRENE»). Le bureau SIRENE servirait de point de contact unique aux États membres pour léchange des informations supplémentaires concernant les signalements.

Les bureaux SIRENE devraient répondre en grande partie aux demandes dinformations supplémentaires au plus tard six heures après leur réception. En cas de signalements dinfractions liées au terrorisme et de signalements concernant des enfants, ils devraient agir immédiatement.

En vue daméliorer la qualité des données dans le SIS, lagence eu-LISA devrait également proposer une formation sur lutilisation du SIS aux organismes nationaux de formation et, dans la mesure du possible, au personnel SIRENE et aux utilisateurs finaux.

Accès au système: la proposition de la Commission prévoit des possibilités daccès renforcées pour une série dagences européennes comme par exemple Europol, Eurojust, et lAgence européenne de garde-frontières et de garde-côtes. Les amendements introduits visent à préciser, en ce qui concerne les mandats existants des différentes agences, les circonstances dans lesquelles il est possible daccéder aux données du SIS.

Il est également proposé de renforcer les garanties à cet égard, que ce soit en termes de formation préalable ou denregistrement dans des journaux ou de surveillance indiquant en particulier, la date et l'heure de l'activité de traitement des données, le type de données traitées et le nom de la personne chargée du traitement des données.

Sécurité des données: les députés ont précisé que les plans nationaux de sécurité, de continuité des opérations et de rétablissement après sinistre devraient permettre: i) dempêcher laccès de toute personne non autorisée au matériel de traitement de données; ii) dempêcher le traitement non autorisé de données introduites dans le SIS ainsi que toute modification ou tout effacement non autorisé de données ; iii) de garantir le rétablissement du système installé en cas dinterruption; iv) de garantir que les erreurs sont signalées et que les données à caractère personnel conservées dans le SIS ne peuvent pas être corrompues par le dysfonctionnement du système.

En vue déviter le piratage du SIS par un prestataire de services extérieur, les députés ont proposé que les États membres qui coopèrent avec des contractants externes sur toute tâche liée au SIS suivent de près les activités des contractants afin de veiller au respect de lensemble des dispositions du règlement notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

Protection des données: laccès au système devrait être subordonné à toutes les dispositions juridiques applicables aux autorités nationales compétentes en matière de protection des données et à la possibilité pour les autorités de contrôle de vérifier la bonne application des dispositions juridiques, notamment par le mécanisme dévaluation de Schengen instauré par le règlement (UE) n° 1053/2013 du Conseil.

Les députés ont proposé une série damendements dans le but de préciser quelles sont les règles applicables. En outre, un certain nombre de dispositions ont été renforcées et mises en conformité avec le cadre européen de protection des données.

Selon le texte amendé, toute introduction et utilisation dans le SIS de photographies, dimages faciales et de données dactyloscopiques devraient i) rester dans les limites de ce qui est strictement nécessaire pour atteindre les objectifs poursuivis, ii) être autorisées par le droit de lUnion, iii) respecter les droits fondamentaux, notamment lintérêt supérieur de lenfant, et iv) être conformes aux dispositions applicables en matière de protection des données prévues par les instruments juridiques du SIS, le règlement (UE) 2016/679 (règlement général sur la protection des données) et la directive (UE) 2016/680 du Parlement européen et du Conseil.

Les données introduites dans le SIS ne devraient pas révéler dinformations sensibles sur la personne, comme lappartenance ethnique, la religion, le handicap, le genre ou lorientation sexuelle.

Signalement aux fins de non-admission: un signalement aux fins de non-admission ou dinterdiction de séjour devrait être délivré après une décision nationale, et uniquement :

- si un ressortissant de pays tiers a été condamné dans un État membre pour une infraction passible dune peine privative de liberté dau

moins trois ans;

- sil y a des raisons sérieuses de croire quun ressortissant dun pays tiers a commis une infraction grave ou un acte terroriste ou sil apparaît quil a lintention de commettre une telle infraction sur le territoire dun État membre.

LÉtat membre devrait prendre une décision administrative ou judiciaire sil conclut, après une évaluation individuelle, que le ressortissant de pays tiers constitue une menace pour lordre public ou la sécurité publique ou pour la sécurité nationale. Ce nest quensuite que lÉtat membre pourrait délivrer le signalement aux fins de non-admission.

Consultation à laide de données biométriques: les députés ont précisé que les données dactyloscopiques stockées dans le SIS ne devraient être utilisées à des fins didentification que si lidentité de la personne ne peut être établie par des données alphanumériques (nom, prénom, date de naissance). À cette fin, le SIS central devrait contenir un système automatisé didentification des empreintes digitales.

Durée de conservation des signalements: le délai fixé pour réexaminer les signalements de personnes devrait être de trois ans au maximum. À titre de principe général, les signalements de personnes devraient être automatiquement supprimés du SIS après trois ans.

Entrée en vigueur des nouvelles dispositions: afin déviter de longs retards, comme ce fut le cas avec le cadre juridique du SIS II, les députés ont proposé que le nouveau cadre juridique soit mis en application un an après son entrée en vigueur.