Système d'information Schengen (SIS) dans le domaine de la coopération policière et judiciaire en matière pénale

2016/0409(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 l' établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant le règlement (UE) n° 515/2014 et abrogeant le règlement (CE) n° 1986/2006, la décision 2007/533/JAI du Conseil et la décision 2010/261/UE de la Commission.

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 d' une copie nationale comprenant une copie complète ou partielle de la base de données du SIS ainsi qu'un 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 proposent qu' une **infrastructure de communication de secours** soit mise au point et soit utilisée en cas de défaillance de l'infrastructure 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 l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace 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 d'assurer l'échange et la disponibilité de toutes les informations supplémentaires (le «bureau SIRENE»). Le **bureau SIRENE** servirait de point de contact unique aux États membres pour l'échange des informations supplémentaires concernant les signalements.

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

En vue d'améliorer la qualité des données dans le SIS, l'agence eu-LISA devrait également proposer **une formation sur l'utilisation 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 d'accès renforcées pour une série d'agences européennes comme par exemple Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes. Les amendements proposés visent à préciser, en ce qui concerne les mandats

existants des différentes agences, les circonstances dans lesquelles il est possible d'accéder aux données du SIS.

Il est également proposé de **renforcer les garanties** à cet égard, que ce soit en termes de formation préalable ou d'enregistrement 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.

Europol devrait être immédiatement informée par les États membres de tous les signalements créés et des réponses positives concernant ces signalements lorsqu'une personne ou un objet est recherché par un État membre en rapport avec une infraction visée dans la directive (UE) 2017/541 relative à la lutte contre le terrorisme.

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) d'empêcher l'accès de toute personne non autorisée au matériel de traitement de données; ii) d'empêcher 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 d'interruption; 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 d'éviter 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 l'ensemble des dispositions du règlement notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

Protection des données: l'accès 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 d'évaluation de Schengen instauré par le règlement (UE) n° 1053/2013 du Conseil.

Les députés ont proposé une série d'amendements 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**, notamment 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 d'informations sensibles** sur la personne, comme l'appartenance ethnique, la religion, le handicap, le genre ou l'orientation sexuelle.

Modifications spécifiques concernant les signalements: les députés ont précisé qu'un signalement devrait être introduit lorsqu'un suspect est recherché en lien avec une **infraction terroriste présumée**. Ils ont également délimité l'utilisation des **données ADN** et défini les circonstances dans lesquelles elles peuvent accompagner un signalement.

Personnes disparues: la catégorie des enfants risquant d'être enlevés, notamment par un membre de la famille, d'être déplacés hors de l'État membre afin de faire l'objet de torture, de violences sexuelles ou fondées sur le genre, ou d'être victimes des activités relevant de la directive (UE) 2017/541 serait introduite dans le SIS.

Un signalement concernant **un enfant en danger** devrait être introduit, à la suite d'une décision de l'autorité judiciaire compétente en matière de responsabilité parentale, lorsque l'enfant risque d'être déplacé, de manière illégale et imminente, hors de l'État membre où se trouve cette autorité judiciaire compétente.

Dans le cas d'enfants disparus faisant l'objet d'un signalement, l'État membre d'exécution devrait consulter l'État membre signalant, et notamment les autorités de protection de l'enfance qui en dépendent, afin de décider au plus tard **dans un délai de 12 heures**, des mesures à prendre pour préserver l'intérêt supérieur de l'enfant.

Les données introduites dans le SIS devraient préciser à quelle catégorie appartient le enfant en danger, à savoir: i) fugueur; ii) **enfant non accompagné dans le contexte des migrations**; iii) enfant enlevé par un membre de la famille.

Contrôles d'investigation: compte tenu de leur nature ceux-ci devraient être obligatoires, en pleine conformité avec l'ensemble des garanties procédurales. Les députés ont **renforcé les exigences** concernant les informations que les États membres sont tenus de fournir pour permettre aux autorités compétentes de l'État membre d'exécution de prendre des mesures. Ces informations devraient être **transmises immédiatement** à l'autorité signalante, lorsque des contrôles ou vérifications aux frontières, des contrôles de police et de douanes ou d'autres actions répressives sont réalisés à l'intérieur d'un État membre.

Entrée en vigueur des nouvelles dispositions: afin d'éviter 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.