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

2016/0408(COD) - 24/10/2018 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 530 voix pour, 50 contre et 66 abstentions, une résolution législative 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 des vérifications aux frontières, modifiant le règlement (UE) n° 515/2014 et abrogeant le règlement (CE) n° 1987/2006.

La position du Parlement européen adoptée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit:

Objectif: le règlement proposé apporterait **une série d'améliorations au SIS** en vue de le rendre plus efficace, de renforcer la protection des données et d'élargir les droits d'accès. Il établirait les conditions et les procédures relatives à l'introduction et au traitement dans le SIS des signalements concernant des ressortissants de pays tiers, et à l'échange d'informations supplémentaires et de données complémentaires aux fins de non-admission et d'interdiction de séjour sur le territoire des États membres.

Architecture du système: le SIS comprend un système central (SIS central) et des systèmes nationaux. Les systèmes nationaux pourraient contenir une copie intégrale ou partielle de la base de données du SIS, qui pourrait être partagée par deux États membres ou plus. La **disponibilité du SIS** ferait l'objet d'un suivi étroit au niveau central et des États membres, et tout cas d'indisponibilité pour les utilisateurs finaux devrait être consigné et signalé aux parties intéressées au niveau national et de l'Union. Chaque État membre devrait mettre en place un **dispositif de secours** pour son système national. L'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (**eu-LISA**) devrait mettre en œuvre des solutions techniques pour renforcer la disponibilité continue du SIS.

Coûts: le texte amendé prévoit que des fonds seraient alloués **à partir de l'enveloppe de 791 millions d' EUR** prévue au règlement (UE) n° 515/2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas, pour couvrir les coûts de mise en œuvre du présent règlement. L'eu-LISA recevrait un montant de 31.098.000 EUR à partir de cette enveloppe, tandis que les États membres recevraient une dotation supplémentaire globale de 36.810.000 EUR à distribuer à parts égales sous la forme de montant forfaitaire s'ajoutant à leur dotation de base.

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.

Chaque bureau SIRENE aurait un **accès facile direct ou indirect** à toutes les informations nationales pertinentes, y compris aux bases de données nationales et à toutes les informations sur les signalements de son État membre afin d'être en mesure de réagir rapidement aux demandes d'informations supplémentaires. Les États membres devraient veiller à ce que les utilisateurs finaux et le personnel des bureaux SIRENE reçoivent régulièrement des **formations**, portant notamment sur la sécurité des données, la protection des données et la qualité des données.

Sécurité des données: le Parlement a précisé que les **plans nationaux de sécurité**, de continuité des opérations et de rétablissement après sinistre devraient permettre i) d'empêcher le **traitement non autorisé** de données dans le SIS et toute modification ou tout effacement non autorisés de données traitées dans le SIS; ii) de garantir le **rétablissement** des systèmes installés en cas d'interruption; iii) de garantir que le SIS exécute correctement ses fonctions, que les erreurs soient signalées et que les **données à caractère personnel** stockées dans le SIS ne puissent pas être corrompues par le dysfonctionnement du système.

Lorsqu'un État membre coopère avec des **prestataires externes** sur toute tâche liée au SIS, il devrait suivre suit de près les activités des prestataires afin de veiller au respect aux dispositions du règlement, notamment en ce qui concerne la sécurité, la confidentialité et la protection des données.

Catégories de données: le texte amendé prévoit l'introduction de nouvelles catégories de données dans le SIS pour permettre aux utilisateurs finaux de prendre des décisions éclairées fondées sur un signalement sans perdre de temps.

En vue de faciliter l'identification et de détecter les identités multiples, le signalement devrait comporter, lorsqu'une telle information est disponible, une référence au **document d'identification personnel** de la personne concernée ou au numéro de ce document et une copie du document, si possible en couleurs. Si elles sont disponibles, toutes les données pertinentes, en particulier le **prénom** de la personne concernée, devraient être insérées lors de la création d'un signalement.

Signalements aux fins de non-admission et d'interdiction de séjour: un signalement ne pourrait être introduit que si l'État membre a pris une décision administrative ou judiciaire et s'il a conclu, après une évaluation individuelle, que le ressortissant de pays tiers constitue une menace pour l'ordre public ou la sécurité publique ou pour la sécurité nationale, à savoir lorsque :

- un ressortissant de pays tiers a été condamné dans un État membre pour une infraction passible d' une **peine privative de liberté d'au moins un an**;
- il y a des raisons sérieuses de croire qu'un ressortissant d'un pays tiers a commis une **infraction pénale grave, y compris un acte terroriste** ou s'il apparaît qu'il a l'intention de commettre une telle infraction sur le territoire d'un État membre;
- un ressortissant de pays tiers a **contourné ou tenté de contourner le droit national ou de l'Union** relatif à l'entrée et au séjour sur le territoire des États membres.

Durée de conservation: dans un délai de **trois ans** à compter de l'introduction d'un signalement dans le SIS, l'État membre signalant devrait réexaminer la nécessité de le conserver. Dans le cas où la décision nationale sur laquelle le signalement se fonde prévoit une durée de validité supérieure à trois ans, le signalement devrait être réexaminé dans un délai de cinq ans.

Données biométriques: en vertu du règlement proposé, le SIS permettrait le traitement des données biométriques afin d'aider à identifier les personnes concernées de manière fiable.

Le Parlement a précisé que toute introduction de photographies, d'images faciales ou de données dactyloscopiques dans le SIS et toute utilisation de ces données devraient i) être **limitées à ce qui est nécessaire** pour atteindre les objectifs poursuivis, ii) être autorisées par le droit de l'Union, iii) respecter les **droits fondamentaux**, notamment l'intérêt supérieur de l'enfant, et iv) être conformes au droit de l'Union en matière de **protection des données**.

Accès au système: le règlement proposé 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.

Afin de pallier le partage insuffisant d'informations sur le terrorisme, en particulier sur les combattants terroristes étrangers, dont la surveillance des mouvements est essentielle, les États membres sont encouragés à **partager avec Europol** leurs informations sur les activités liées au terrorisme. Ce partage d'informations devrait s'effectuer par la voie d'échange d'informations supplémentaires avec Europol sur les signalements concernés.