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

2016/0409(COD) - 24/10/2018 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 555 voix pour, 67 contre et 20 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 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 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 personnes ou des objets**, et à l'échange d'informations supplémentaires et de données complémentaires aux fins de la coopération policière et de la coopération judiciaire en matière pénale.

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.

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: les députés ont 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: les signalements concernant les catégories suivantes de personnes seraient introduits dans le SIS à la demande de l'autorité compétente de l'État membre signalant:

- **les personnes disparues** qui doivent être placées sous protection pour prévenir une menace à l'ordre public ou à la sécurité publique;
- **les enfants risquant d'être enlevés** par un de leurs parents, un membre de leur famille ou un tuteur, qui doivent être empêchés de voyager;
- **les enfants qui doivent être empêchés de voyager** en raison du risque manifeste qu'ils courent d' être déplacés hors du territoire d'un État membre et i) de devenir victimes de la traite des êtres humains, ou d'un mariage forcé, d'une mutilation génitale féminine ou de toute autre forme de violence fondée sur le genre; ii) de devenir victimes d'infractions terroristes ou d'être impliqués dans de telles infractions; iii) de subir l'enrôlement dans des groupes armés;
- **les personnes vulnérables majeures** et qui doivent être empêchées de voyager dans l'intérêt de leur propre protection en raison du risque concret et manifeste qu'elles courent d'être déplacées hors du territoire d'un État membre et de devenir victimes de la traite des êtres humains ou de violences fondées sur le genre.

Les mesures et décisions prises par les autorités compétentes, notamment les autorités judiciaires, à la suite d'un signalement concernant un enfant devraient être prises en concertation avec les autorités responsables de la protection de l'enfance. Si nécessaire, la ligne nationale d'urgence pour les disparitions d'enfants devrait en être informée.

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.

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.

Il serait également possible d'ajouter un **profil ADN** à un signalement dans des cas clairement définis où l'on ne dispose pas de données dactyloscopiques. Ce profil ADN ne devrait être accessible qu'à des utilisateurs autorisés.

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. Les amendements adoptés 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.