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

2016/0409(COD) - 21/12/2016 - Document de base législatif

OBJECTIF : reformer le Système d'Information Schengen (SIS) afin de renforcer le cadre général de la coopération policière et judiciaire en matière pénale, modifier consécutivement le règlement (UE) n° 515 /2014 et abroger le règlement (CE) n° 1986/2006, la décision du Conseil 2007/533/JAI et la décision de la Commission 2010/261/UE.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide, conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : en 2016, la Commission a procédé à une évaluation complète du SIS, 3 ans après l'entrée en vigueur de la mise en place de sa 2ème génération. Cette évaluation a montré que le SIS était pleinement opérationnel.

Néanmoins, des efforts s'avèrent encore nécessaires et c'est pourquoi, la Commission présente une série de propositions visant à améliorer et étendre l'utilisation du SIS, tout en poursuivant ses travaux pour rendre plus interopérables les systèmes existants en matière de gestion des frontières.

Ces propositions portent plus précisément sur l'utilisation du système pour assurer :

- la gestion des frontières,
- la coopération policière et la coopération judiciaire en matière pénale (qui fait l'objet de la présente proposition), et
- le retour des ressortissants de pays tiers en séjour irrégulier.

CONTENU : la présente proposition et la proposition complémentaire sur la gestion des frontières, visent à fixer les règles couvrant **l'exploitation complète du système**, y compris le SIS central géré par l' Agence eu-LISA, les systèmes nationaux et les applications des utilisateurs finaux.

**Utilisateurs** : avec plus de 2 millions d'utilisateurs finaux à travers l'Europe, le SIS est un outil très largement utilisé et efficace pour l'échange d'informations. La présente proposition et la proposition parallèle sur la gestion des frontières comprennent des règles couvrant l'exploitation complète du système, y compris le SIS central géré par l'Agence eu-LISA, les systèmes nationaux et les applications des utilisateurs finaux.

Afin d'utiliser pleinement le SIS, les États membres devraient veiller à ce que chaque fois que leurs utilisateurs finaux doivent effectuer une recherche dans une base de données nationale de police ou d'immigration, ils fassent également une recherche parallèle dans le SIS. De cette manière, le SIS pourra remplir son objectif en tant que **principale mesure compensatoire à la liberté de circulation dans un espace sans frontières intérieures** et faire en sorte que les États membres puissent mieux traiter la dimension transfrontalière de la criminalité et la mobilité des criminels.

**Qualité des données** : la proposition maintient le principe selon lequel l'État membre, qui est le propriétaire des données, est également responsable de l'exactitude des données saisies dans le SIS. Il est toutefois prévu de mettre en place un mécanisme central géré par eu-LISA, qui permettra aux États membres d'examiner régulièrement les alertes qui font l'objet d'un problème de qualité.

A cet effet, l'Agence eu-LISA devra produire à intervalles réguliers des rapports sur la qualité des données à destination des États membres.

**Photographies, images faciales, empreintes digitales, empreintes palmaires et profils ADN** : la possibilité de rechercher des empreintes digitales en vue d'identifier une personne est déjà prévue dans la règlementation existante. Les deux nouvelles propositions rendent cette recherche **obligatoire** si l'identité de la personne ne peut être établie d'aucune autre manière.

Actuellement, les images faciales ne peuvent être utilisées que pour confirmer l'identité d'une personne suite à une recherche alphanumérique, plutôt que comme base de recherche. Avec les modifications prévues à la présente proposition, il est prévu que les images faciales, les photographies et **les empreintes palmaires** soient utilisés pour effectuer des recherches dans le système et permettent d'identifier les personnes, lorsque cela est techniquement possible (en plus des empreintes digitales).

Dans les cas où les empreintes digitales ou les empreintes palmaires ne sont pas disponibles, la proposition permet l'utilisation de profils ADN pour les personnes disparues qui doivent être placées sous protection, en particulier les enfants. Cette fonctionnalité ne sera utilisée qu'en l'absence d'empreintes digitales et ne sera accessible qu'aux utilisateurs autorisés.

Les modifications proposées permettront également de **diffuser des alertes SIS pour les personnes suspectées de crime mais non répertoriées** et dont les empreintes digitales ou palmaires ont été relevées. Cette nouvelle catégorie d'alerte complète les dispositions du mécanisme de Prüm qui permet l'interconnexion des systèmes nationaux d'identification des empreintes digitales criminelles. Par le biais de ce mécanisme, un État membre pourra introduire une demande visant à déterminer si l'auteur d'un crime dont les empreintes digitales ont été relevées, **est connu dans tout autre État membre**.

Toutefois, ce type de comparaison ne peut intervenir que si une personne a vu ses empreintes digitales relevées à la suite d'un crime. Par conséquent**, les délinquants qui sont interpellés pour la première fois ne peuvent être identifiés**.

Avec la présente proposition, et **le stockage des empreintes digitales de personnes recherchées et non répertoriées**, il deviendra possible de transférer les empreintes digitales d'un auteur inconnu dans le SIS afin qu'il puisse être identifié, s'il a été interpellé dans un autre État membre.

A noter toutefois que l'utilisation de cette fonctionnalité ne pourra intervenir que si les États membres ont procédé à une consultation préalable de toutes les sources nationales et internationales disponibles, sans pouvoir déterminer l'identité de la personne concernée.

**Accès des autorités responsables de l'immigration au SIS - utilisateurs institutionnels** : des dispositions nouvelles décrivent **les droits d'accès à l'égard des agences de l'UE** (utilisateurs institutionnels) telles qu'Europol, Eurojust ou l'Agence européenne pour la gestion des frontières.

Des garanties appropriées sont mises en place pour que les données du système soient correctement protégées exigeant que ces organismes puissent uniquement accéder aux données dont ils ont besoin pour mener à bien leurs tâches.

Des dispositions sont également prévues pour permettre aux autorités responsables de l'immigration d' accéder au SIS.

**Blocage de certaines alertes** : des dispositions sont prévues pour permettre aux États membres de suspendre temporairement certaines alertes en vue d'une arrestation (en cas d'opération policière ou d'une enquête notamment), les rendant visibles uniquement aux bureaux SIRENE mais pas aux agents sur le terrain pendant une période limitée dans le temps. Cette disposition est prévue pour éviter qu'une opération de police confidentielle visant à arrêter un suspect soit menacée par un policier qui n'est pas impliqué par cette opération.

De même, des dispositions ont été prévues pour prévenir **les enlèvements parentaux**. Ainsi, il sera désormais possible d'établir des **alertes spécifiques et préventives** pour des enfants présentant un haut risque d'enlèvement parental. Dans ce cas, les gardes-frontières et les responsables de l'application de la loi seront sensibilisés au risque d'enlèvement, en cas de passage à la frontière du parent concerné et pourront examiner de plus près les circonstances dans lesquelles un enfant qui voyage avec ce parent peut présenter un risque. Ces autorités pourraient être amenées à mettre le parent concerné en garde à vue si nécessaire.

**Contrôle d'enquête** : une nouvelle forme de contrôle est introduite, le «contrôle lié à une enquête» en lien avec la lutte contre le terrorisme et la criminalité grave. Il permet aux autorités d'arrêter et d'interroger une personne suspecte. Cela va au-delà d'une opération de contrôle discret, sans pour autant se résumer à une arrestation pure et simple.

D'autres types d'alertes sont envisagés pour des documents vierges, des documents liés à des véhicules ou des bateaux afin de favoriser la vérification de documents qui semblent *a priori* authentiques mais sont, par exemple, utilisés par plusieurs utilisateurs en même temps.

D'autres alertes encore ont été ajoutées pour des équipements IT, des faux billets, des pièces détachées, etc.

**Protection et sécurité des données** : des dispositions sont insérées pour clarifier la responsabilité de la prévention, de la notification et de la réponse aux incidents susceptibles d'affecter la sécurité ou l'intégrité de l'infrastructure SIS, des données du SIS ou les informations complémentaires.

En termes de responsabilité notamment, il est prévu que la Commission reste responsable de la gestion contractuelle de l'infrastructure de communication du SIS avec un certain nombre de tâches dévolues à l' Agence eu-LISA.

**Catégories de données et traitement de données** : afin de fournir aux utilisateurs finaux des informations de plus en plus précises pour faciliter et accélérer les actions requises ainsi que pour permettre une meilleure identification des alertes, la proposition élargit les types d'informations auxquelles il sera possible d'accéder.

La proposition élargit également la liste des données à caractère personnel qui peuvent être saisies et traitées dans le SIS. Il est en effet essentiel d'avoir des données appropriées pour assurer l'identification exacte d'une personne contrôlée à un poste frontière et qui demande l'autorisation de séjour sur le territoire des États membres. Cela est également essentiel pour éviter des problèmes **d'usurpation d'identité**.

Désormais, le SIS pourra inclure:

- des images faciales;
- des empreintes palmaires;

- des détails liés aux documents d'identité;
- l'adresse de la victime d’une usurpation d’identité;
- les noms du père et de la mère de la victime.

Des dispositions listent en outre (comme avant) les droits des personnes pouvant accéder aux données du SIS et la possibilité de rectifier les données inexactes ou effacer les données stockées illégalement.

En outre des dispositions sont prévues en matière de rétention des données (en règle générale, 5 ans sauf pour certaines recherches spécifiques de type discrète et dont la rétention devrait se limiter à un an).

Enfin, des dispositions sont prévues en matière de statistiques sur le recours au SIS.

INCIDENCE BUDGÉTAIRE : le coût de la mesure est estimé à **64,3 millions EUR** de 2018 à 2020.