Informations de base

2016/0409(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	Procédure terminée
Système d'information Schengen (SIS) dans le domaine de la coopération policière et judiciaire en matière pénale Abrogation Décision 2007/533/JHA 2005/0103(CNS) Abrogation Règlement (EC) No 1986/2006 2005/0104(COD) Modification 2018/0152B(COD) Modification 2019/0001A(COD) Modification 2019/0001B(COD) Voir aussi 2016/0408(COD) **Subject** 7.10.04 Franchissement et contrôles aux frontières extérieures, visas 7.30.05 Coopération policière 7.40.04 Coopération judiciaire en matière pénale	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
LIBE Libertés civiles, justice et affaires intérieures	COELHO Carlos (PPE)	09/03/2017
	Rapporteur(e) fictif/fictive DALLI Miriam (S&D) HALLA-AHO Jussi (ECR) DEPREZ Gérard (ALDE) VERGIAT Marie-Christine (GUE/NGL) JOLY Eva (Verts/ALE) MEUTHEN Jörg (EFDD) FONTANA Lorenzo (ENF)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	La commission a décidé de ne pas donner d'avis.	
BUDG Budgets	La commission a décidé de ne pas donner d'avis.	

TRAN Transports et tourisme	La commission a décidé de ne pas donner d'avis.	
JURI Affaires juridiques	La commission a décidé de ne pas donner d'avis.	

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Transports, télécommunications et énergie	3545	2017-06-09
Agriculture et pêche	3651	2018-11-19

Commission européenne

DG de la Commission	Commissaire
Migration et affaires intérieures	AVRAMOPOULOS Dimitris

Evénements clés

Date	Evénement	Référence	Résumé
21/12/2016	Publication de la proposition législative	COM(2016)0883	Résumé
06/04/2017	Annonce en plénière de la saisine de la commission, 1ère lecture		
09/06/2017	Débat au Conseil		
19/10/2017	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
06/11/2017	Vote en commission,1ère lecture		
06/11/2017	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
10/11/2017	Dépôt du rapport de la commission, 1ère lecture	A8-0349/2017	Résumé
13/11/2017	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
15/11/2017	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
23/10/2018	Débat en plénière		
24/10/2018	Décision du Parlement, 1ère lecture	T8-0413/2018	Résumé
24/10/2018	Résultat du vote au parlement		
19/11/2018	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
28/11/2018	Signature de l'acte final		
28/11/2018	Fin de la procédure au Parlement		
07/12/2018	Publication de l'acte final au Journal officiel		

Informations techniques	
Référence de la procédure	2016/0409(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Règlement
Modifications et abrogations	Abrogation Décision 2007/533/JHA 2005/0103(CNS) Abrogation Règlement (EC) No 1986/2006 2005/0104(COD) Modification 2018/0152B(COD) Modification 2019/0001A(COD) Modification 2019/0001B(COD) Voir aussi 2016/0408(COD)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 085-p1-a3 Traité sur le fonctionnement de l'UE TFEU 088-p2-a2 Traité sur le fonctionnement de l'UE TFEU 082-p1 Traité sur le fonctionnement de l'UE TFEU 087-p2
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/8/08847

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE606.235	27/06/2017	
Amendements déposés en commission		PE609.654	07/09/2017	
Amendements déposés en commission		PE610.562	07/09/2017	
Rapport déposé de la commission, 1ère lecture/lecture unique		A8-0349/2017	10/11/2017	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T8-0413/2018	24/10/2018	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Projet d'acte final	00036/2018/LEX	28/11/2018	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2016)0883	21/12/2016	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2018)755	21/11/2018	
Document de suivi	COM(2020)0072	28/02/2020	
	COM(2021)0336		

Document de suivi		29/06/2021	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	ES_PARLIAMENT	COM(2016)0883	23/05/2017	
Contribution	PT_PARLIAMENT	COM(2016)0883	29/05/2017	
Contribution	IT_SENATE	COM(2016)0883	06/06/2017	
Contribution	CZ_SENATE	COM(2016)0883	13/06/2017	
Contribution	IT_CHAMBER	COM(2016)0883	04/08/2017	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EDPS	Document annexé à la procédure	N8-0046/2017 JO C 200 23.06.2017, p. 0014	03/05/2017	

Informations complémentaires

Source	Document	Date
Service de recherche du PE	Briefing	

Acte final

Règlement 2018/1862
JO L 312 07.12.2018, p. 0056 Résumé

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.

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.

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.

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

2016/0409(COD) - 28/11/2018 - Acte final

OBJECTIF : améliorer le Système d'information Schengen (SIS) dans le domaine de la coopération policière et judiciaire en matière pénale en vue de le rendre plus efficace, de renforcer la protection des données et d'élargir les droits d'accès.

ACTE LÉGISLATIF : Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 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 et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission.

CONTENU : le système d'information Schengen (SIS) constitue un outil essentiel pour l'application des dispositions de l'acquis de Schengen tel qu'il a été intégré dans le cadre de l'Union européenne. Le présent règlement :

- établit 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 ;

- prévoit des dispositions concernant l'architecture technique du SIS, les responsabilités incombant aux États membres et à 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»), le traitement des données, les droits des personnes concernées et la responsabilité.

Le règlement s'accompagne de deux autres règlements relatifs à l'utilisation du SIS : i) dans le domaine de la vérification aux frontières ; ii) aux fins du retour des ressortissants de pays tiers en séjour irrégulier.

Architecture

Le SIS comprend un système central (SIS central) et des systèmes nationaux. Les systèmes nationaux pourront contenir une copie intégrale ou partielle de la base de données du SIS, qui peut être partagée par deux États membres ou plus. Le SIS central et l'infrastructure de communication de devront être gérées manière à assurer leur fonctionnement 24 heures sur 24, 7 jours sur 7. Pour cette raison, l'agence « eu-LISA» devra mettre en œuvre des solutions techniques pour renforcer la disponibilité continue du SIS.

Nouvelles catégories de signalements

Seront dorénavant introduits dans le système:

- les signalements émis aux fins de contrôles d'investigation, une étape intermédiaire entre les contrôles discrets et les contrôles spécifiques, qui permettent d'interroger les personnes concernées;

- les signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise sur la base d'un mandat d'arrêt européen ou les signalements concernant des personnes recherchées en vue d'une arrestation aux fins d'extradition ;

- les signalements préventifs relatifs aux enfants risquant d'être enlevés par un parent ainsi qu'aux enfants et aux personnes vulnérables qu'il y a lieu d'empêcher de voyager dans l'intérêt de leur propre protection (par exemple lorsque le voyage peut entraîner un risque de mariage forcé, de mutilation sexuelle féminine, de trafic d'êtres humains).

S'il s'agit d'enfants, toute décision sur les mesures à prendre ou toute décision de placement de l'enfant en lieu sûr devra être prise dans le respect de l'intérêt supérieur de l'enfant. Ces décisions devront être prises immédiatement et au plus tard dans un délai de 12 heures suivant le moment où l'enfant a été localisé, en concertation avec les autorités responsables de la protection de l'enfance concernées, s'il y a lieu.

Le règlement permet également l'introduction de signalements concernant des objets aux fins d'une saisie ou à titre de preuve dans une procédure pénale comme par exemple les faux documents et les objets identifiables de grande valeur, ainsi que le matériel informatique.

Nouvelles catégories de données

Le règlement 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.

Afin de faciliter l'identification et de détecter les identités multiples, le signalement devra comporter, si l'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, devront être insérées lors de la création d'un signalement.

Données biométriques

Le SIS permettra le traitement des données biométriques afin d'aider à identifier les personnes concernées de manière fiable. Toute introduction de photographies, d'images faciales ou de données dactyloscopiques dans le SIS et toute utilisation de ces données devront 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.

En vue d'éviter les problèmes causés par des erreurs d'identification, le SIS permettra également le traitement de données relatives à des personnes dont l'identité a été usurpée, sous réserve de garanties adaptées, de l'obtention du consentement des personnes concernées pour chaque catégorie de données, en particulier les empreintes palmaires, et d'une stricte limitation des fins auxquelles ces données à caractère personnel peuvent être traitées de manière licite.

Accès aux données

Europol aura accès à toutes les catégories de données figurant dans le SIS et pourra échanger des informations supplémentaires avec les bureaux SIRENE des États membres. En outre, les États membres doivent informer Europol de toute réponse positive lorsqu'une personne est recherchée dans le cadre d'une infraction terroriste. L'Agence européenne de garde-frontières et de garde-côtes aura également accès aux différentes catégories de signalements figurant dans le SIS.

ENTRÉE EN VIGUEUR : 27.12.2018.

Au plus tard le 28.12.2021, la Commission adoptera une décision fixant la date à laquelle le SIS est mis en service en vertu du règlement, après avoir vérifié que les conditions sont remplies.