

Bruxelles, le 13 novembre 2017
(OR. en)

14116/17

**Dossier interinstitutionnel:
2016/0409 (COD)**

**SIRIS 189
ENFOPOL 514
COPEN 335
SCHENGEN 80
COMIX 748
CODEC 1769**

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
N° doc. préc.:	13454/17
N° doc. Cion:	15814/16
Objet:	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 - Mandat autorisant l'ouverture de négociations interinstitutionnelles

Lors de sa réunion du 8 novembre 2017, le Coreper a décidé de donner mandat à la présidence pour ouvrir des négociations interinstitutionnelles sur la base du texte de compromis révisé qui figure en annexe.

Une déclaration de la Grèce sera annexée au procès-verbal de la réunion du Coreper du 8 novembre 2017.

Cet instrument fait toujours l'objet d'une réserve générale et d'une réserve d'examen parlementaire de la délégation du Royaume-Uni.

Les modifications apportées par rapport à la proposition initiale de la Commission sont indiquées comme suit: les passages nouveaux ou modifiés figurent en **caractères gras soulignés**; les passages supprimés sont signalés par des crochets [...].

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**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, second alinéa, point d), son article 85, paragraphe 1, son article 87, paragraphe 2, point a), et son article 88, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

- (1) Le système d'information Schengen (ci-après dénommé "SIS") constitue un outil essentiel pour l'application des dispositions de l'acquis de Schengen, intégré dans le cadre de l'Union européenne. Il représente l'une des grandes mesures compensatoires **et l'un des grands instruments répressifs** qui contribuent au maintien d'un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne par le soutien qu'il apporte à la coopération opérationnelle entre les garde-frontières, la police, les douanes et les autres autorités [...] **chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes et des poursuites en la matière ou de l'exécution des sanctions pénales et des vérifications portant sur les ressortissants de pays tiers** [...] ¹.

¹ Libellé correspondant à celui de l'article 43, paragraphe 1, point c).

- (2) Le SIS a **initialement** été créé conformément aux dispositions du titre IV de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes² (convention de Schengen), signée le 19 juin 1990. La Commission a été chargée, par le règlement (CE) n° 2424/2001 du Conseil³ et la décision 2001/886/JAI du Conseil⁴, du développement du SIS de deuxième génération (SIS II), qui a été créé par le règlement (CE) n° 1987/2006⁵ et la décision 2007/533/JAI du Conseil⁶. Le SIS II a remplacé le SIS tel qu'il avait été créé par la convention de Schengen.
- (3) Trois ans après l'entrée en service du SIS II, la Commission a procédé à une évaluation du système, comme le prescrivaient l'article 24, paragraphe 5, l'article 43, paragraphe 3, et l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi que l'article 59 et l'article 66, paragraphe 5, de la décision 2007/533/JAI. Le rapport d'évaluation et le document de travail des services de la Commission qui lui était lié ont été adoptés le 21 décembre 2016⁷. [...] **L**es recommandations formulées dans ces documents **sont** prises en compte, lorsqu'il y a lieu, dans le présent règlement.

² JO L 239 du 22.9.2000, p. 19. Convention modifiée par le règlement (CE) n° 1160/2005 du Parlement européen et du Conseil (JO L 191 du 22.7.2005, p. 18).

³ JO L 328 du 13.12.2001, p. 4.

⁴ Décision 2001/886/JAI du Conseil du 6 décembre 2001 relative au développement du système d'information de Schengen de deuxième génération (SIS II) (JO L 328 du 13.12.2001, p. 1).

⁵ Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28.12.2006, p. 4).

⁶ Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 205 du 7.8.2007, p. 63).

⁷ Rapport d'évaluation du système d'information Schengen de deuxième génération (SIS II) présenté au Parlement européen et au Conseil conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006 ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI, et document de travail des services de la Commission l'accompagnant.

- (4) Le présent règlement constitue la base législative requise pour régir le SIS dans les domaines relevant du titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne. Le règlement (UE) 2018/... 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 frontières⁸ constitue la base législative requise pour régir le SIS dans les domaines relevant du champ d'application du titre V, chapitre 2, du traité sur le fonctionnement de l'Union européenne.
- (5) Le fait que la base législative requise pour régir le SIS consiste en des instruments distincts n'affecte pas le principe selon lequel le SIS constitue un système d'information unique qui devrait fonctionner en tant que tel **et comprendre un réseau unique de bureaux SIRENE pour assurer l'échange d'informations supplémentaires**. Certaines dispositions de ces instruments devraient donc être identiques.
- (6) Il est nécessaire de préciser les objectifs du SIS, **certaines éléments de** son architecture technique et son financement, de fixer des règles concernant son fonctionnement et son utilisation "de bout en bout" et de définir les responsabilités y afférentes, ainsi que les catégories de données à introduire dans le système, les finalités de leur introduction **et de leur traitement**, les critères de leur introduction, les autorités qui sont autorisées à y avoir accès, l'utilisation [...] **de données** biométriques, et d'autres règles relatives au traitement des données.

⁸ Règlement (UE) 2018/...

- (7) Le SIS comprend un système central (SIS central) et des systèmes nationaux, **qui peuvent comporter** [...] une copie intégrale ou partielle de la base de données du SIS **pouvant être partagée par deux ou plusieurs États membres**. Étant donné qu'il est l'instrument d'échange d'informations le plus important en Europe **pour assurer la sécurité et une gestion efficace des flux migratoires**, il est indispensable de garantir son fonctionnement ininterrompu au niveau tant central que national. **La disponibilité du SIS devrait faire 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'UE.** [...] Chaque État membre devrait [...] mettre en place **un** [...] dispositif de secours **pour son** système **national**. **Les États membres devraient également garantir une connectivité ininterrompue avec le SIS central en prévoyant des points de connexion doubles qui soient physiquement et géographiquement séparés. Il convient de gérer le SIS central de manière à assurer son fonctionnement 24 heures sur 24, sept jours sur sept. Une solution actif-actif peut être utilisée à cette fin.**
- (7 bis) L'architecture technique du SIS peut faire l'objet de modifications à la suite de développements techniques, étant entendu qu'il y a lieu d'assurer le degré de disponibilité le plus élevé possible pour les utilisateurs finaux au niveau tant central que national, le respect de toutes les obligations applicables en matière de protection des données, les services nécessaires à l'introduction et au traitement des données dans le SIS, y compris les consultations dans la base de données du SIS, ainsi qu'un réseau de communication virtuel crypté consacré aux données du SIS et l'échange de données entre les bureaux SIRENE. Les modifications devraient être décidées sur la base d'une analyse d'impact et des coûts et seront communiquées au Parlement européen et au Conseil.**
- (8) Il est nécessaire de disposer d'un manuel qui contienne des règles détaillées sur l'échange [...] d'informations supplémentaires concernant la conduite à tenir à la suite de signalements. Les autorités nationales de chaque État membre (bureaux SIRENE) devraient assurer cet échange d'informations.

- (9) En vue de l'échange efficace d'informations supplémentaires [...], il y a lieu de renforcer le fonctionnement des bureaux SIRENE en précisant les besoins en matière de ressources disponibles, de formation des utilisateurs et de délai de réponse aux demandes de renseignements reçues d'autres bureaux SIRENE.
- (10) 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 justice⁹ (ci-après dénommée "agence eu-LISA") est chargée de la gestion opérationnelle des éléments centraux du SIS. Afin de permettre à l'agence eu-LISA de consacrer les moyens financiers et humains nécessaires pour couvrir tous les aspects de la gestion opérationnelle du SIS central **et de l'infrastructure de communication**, le présent règlement devrait décrire ses tâches en détail, notamment pour les aspects techniques de l'échange d'informations supplémentaires.
- (11) Sans préjudice de la responsabilité **principale** des États membres relative à l'exactitude des données introduites dans le SIS **et du rôle des bureaux SIRENE en tant que coordinateurs de la qualité**, l'agence eu-LISA devrait être chargée de renforcer la qualité des données en introduisant un outil de contrôle central de cette qualité et de présenter des rapports réguliers **à la Commission et** aux États membres.
- (12) En vue d'un meilleur contrôle de l'utilisation du SIS pour analyser les tendances dans les infractions pénales, l'agence eu-LISA devrait être en mesure d'acquérir une capacité moderne et performante lui permettant de fournir des rapports statistiques aux États membres, à la Commission, à Europol et à l'Agence européenne de garde-frontières et de garde-côtes sans compromettre l'intégrité des données. Il conviendrait dès lors de créer un fichier statistique central. Les statistiques produites ne devraient pas contenir de données à caractère personnel. **Les États membres devraient communiquer par l'intermédiaire du mécanisme de coopération des statistiques concernant le droit d'accès, de rectification des données inexactes et d'effacement des données stockées illégalement.**

⁹ Instituée par le règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une 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 (JO L 286 du 1.11.2011, p. 1).

(13) Le SIS devrait contenir d'autres catégories de données pour permettre aux utilisateurs finaux de prendre des décisions éclairées fondées sur un signalement sans perdre de temps. En conséquence, afin de faciliter l'identification des personnes et de détecter les identités multiples, les catégories de données relatives aux personnes devraient comporter une référence au document ou numéro d'identification personnel et une copie de ce document, si elle est disponible.

(13 bis) Si elles sont disponibles, toutes les données pertinentes, en particulier le prénom, devraient être insérées lors de la création d'un signalement, afin de réduire autant que possible le risque de fausses réponses positives et les activités opérationnelles inutiles.

(14) Le SIS ne devrait pas stocker de données ayant servi à des consultations, sauf les journaux conservés afin de pouvoir contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS, ainsi que l'intégrité et la sécurité des données.

(15) Le SIS devrait permettre le traitement des données biométriques afin d'aider à l'identification correcte des personnes concernées. À cet égard, le SIS devrait également permettre le traitement de données relatives à des personnes dont l'identité a été usurpée (de manière à éviter les problèmes que pourraient causer des erreurs d'identification), sous réserve de garanties adaptées, en particulier le consentement des personnes concernées et une stricte limitation des fins auxquelles ces données peuvent être licitement traitées.

- (16) Les États membres devraient prendre les mesures techniques nécessaires pour que, chaque fois que les utilisateurs finaux ont le droit de consulter une base de données nationale des services de police ou d'immigration, ils puissent aussi consulter le SIS en parallèle, conformément à l'article 4 de la directive (UE) 2016/680 du Parlement européen et du Conseil¹⁰. Le SIS serait ainsi la principale mesure compensatoire dans l'espace sans contrôles aux frontières intérieures et tiendrait mieux compte de la dimension transfrontière de la criminalité et de la mobilité des criminels.
- (17) Le présent règlement devrait définir les conditions d'utilisation des données [...] **dactyloscopiques** et des images faciales à des fins d'identification. Le recours aux images faciales pour identifier des personnes dans le SIS devrait **en particulier** [...] contribuer à assurer la cohérence des procédures de contrôle aux frontières dans lesquelles l'identification et la vérification de l'identité doivent être réalisées à l'aide des empreintes **dactyloscopiques** [...] et des images faciales. Une consultation à l'aide des données [...] **dactyloscopiques** devrait être obligatoire s'il y a le moindre doute sur l'identité d'une personne. [...]

¹⁰ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

(18) L'introduction d'un système de reconnaissance automatisée d'empreintes digitales dans le SIS complète l'actuel dispositif fondé sur le traité de Prüm sur l'accès mutuel transfrontière en ligne à certaines bases de données nationales de profils ADN et à certains systèmes nationaux de reconnaissance automatisée d'empreintes digitales¹¹. Le dispositif fondé sur le traité de Prüm permet d'interconnecter les systèmes nationaux de reconnaissance d'empreintes digitales et un État membre peut ainsi les interroger pour vérifier si l'auteur d'une infraction dont les empreintes digitales ont été trouvées est connu dans un autre État membre. Cependant, ce dispositif vérifie seulement si le propriétaire des empreintes digitales est connu à un moment donné. [...] **Par conséquent**, si l'auteur de l'infraction ne vient à être connu dans un État membre que plus tard, il pourra passer entre les mailles du filet. La consultation à l'aide des empreintes digitales dans le SIS permet une recherche active de l'auteur d'une infraction. Il devrait donc être possible de charger dans le SIS les empreintes d'un auteur inconnu, à condition que la personne à laquelle appartiennent les empreintes puisse être identifiée avec un degré élevé de probabilité comme l'auteur d'une infraction grave ou d'un acte de terrorisme. Ce serait notamment le cas si des empreintes étaient trouvées sur l'arme ou sur tout objet ayant servi à commettre l'infraction. La seule présence des empreintes sur le lieu de l'infraction ne devrait toutefois pas être considérée comme indiquant, avec un degré élevé de probabilité, que ces empreintes sont celles de l'auteur de l'infraction. Une autre condition préalable à la création d'un tel signalement devrait être que l'identité de l'auteur de l'infraction ne puisse être établie en recourant aux autres bases de données nationales, européennes ou internationales. Si la consultation à l'aide des empreintes digitales aboutit à une correspondance potentielle, l'État membre devrait procéder à d'autres vérifications d'empreintes, [...] avec la participation d'experts en la matière, pour déterminer si les empreintes stockées dans le SIS appartiennent à la personne, et il devrait établir l'identité de celle-ci. Les procédures devraient être régies par le droit national. Le fait d'identifier une "personne recherchée inconnue" dans le SIS peut faire avancer considérablement une enquête et aboutir à une arrestation, pour autant que toutes les conditions de cette dernière soient remplies.

¹¹ Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 1); et décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 12).

- (19) Les empreintes digitales **ou palmaires** trouvées sur le lieu d'une infraction devraient pouvoir être comparées aux **données dactyloscopiques** [...] stockées dans le SIS s'il peut être établi avec un degré élevé de probabilité qu'elles sont celles de l'auteur de l'infraction grave ou de l'infraction terroriste. **Il convient d'accorder une attention particulière à l'établissement de normes de qualité applicables au stockage de données biométriques, y compris les données dactyloscopiques latentes.** Les "infractions graves" devraient correspondre aux infractions énumérées dans la décision-cadre 2002/584/JAI du Conseil¹² et les "infractions terroristes" aux infractions [...] **qui correspondent ou sont équivalentes à l'une des infractions** visées dans **la directive (UE) 2017/541**¹³. [...] ¹⁴
- (20) Il devrait être possible d'ajouter, dans les cas où les données [...] **dactyloscopiques, des photographies ou des images faciales** ne sont pas disponibles, un profil ADN qui ne serait accessible qu'aux utilisateurs autorisés. Les profils ADN devraient faciliter l'identification des personnes disparues qui ont besoin d'une protection, et en particulier des enfants disparus, notamment si l'on autorise l'utilisation des profils ADN **des ascendants, des descendants** [...] ou des frères et sœurs pour permettre l'identification. Les données ADN ne devraient pas faire mention de l'origine raciale.
- (20 bis) Il devrait être possible dans tous les cas d'identifier une personne en utilisant des données dactyloscopiques. Lorsque l'identité de la personne ne peut être établie par aucun autre moyen, il convient d'utiliser les données dactyloscopiques pour tenter d'établir cette identité.**
- (20 ter) Les profils ADN ne devraient être extraits du SIS que lorsqu'une identification est nécessaire et proportionnée aux fins de l'article 32, paragraphe 2, points a) et c). Les profils ADN ne devraient être extraits du SIS et traités à aucune autre fin que celles pour lesquelles ils ont été introduits conformément à l'article 32, paragraphe 2, points a) et c). Dans le respect des règles de protection et de sécurité des données fixées dans le présent règlement, des garanties supplémentaires devraient, si nécessaire, être mises en place lors de l'utilisation de profils ADN afin de prévenir les risques de fausses correspondances, de piratage et de communication non autorisée à des tiers.**

¹² Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

¹³ Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

¹⁴ [...]

- (21) Le SIS devrait contenir des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise et en vue d'une arrestation aux fins d'extradition. Outre les signalements, il convient de prévoir l'échange, **par l'intermédiaire des bureaux SIRENE**, d'informations supplémentaires nécessaires aux procédures de remise et d'extradition. En particulier, les données visées à l'article 8 de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres¹⁵ devraient être traitées dans le SIS. Pour des raisons opérationnelles, il convient que l'État membre signalant, avec l'autorisation des autorités judiciaires, rende temporairement non consultable un signalement aux fins d'arrestation existant lorsqu'une personne qui fait l'objet d'un mandat d'arrêt européen est intensivement et activement recherchée et que les utilisateurs finaux qui ne participent pas aux opérations de recherche risquent de compromettre leur succès. L'impossibilité temporaire de consulter ces signalements ne devrait **en principe** pas dépasser 48 heures.
- (22) Il faudrait prévoir la possibilité d'ajouter dans le SIS une traduction des données complémentaires introduites aux fins de remise en vertu d'un mandat d'arrêt européen et aux fins d'extradition.
- (23) Le SIS devrait contenir des signalements concernant les personnes disparues ou **vulnérables** afin d'assurer leur protection ou de prévenir des menaces contre la sécurité publique. La possibilité d'introduire un signalement dans le SIS pour les enfants risquant d'être enlevés (c'est-à-dire pour prévenir un futur fait dommageable qui n'a pas encore eu lieu, comme c'est le cas pour les risques d'enlèvement parental d'enfants) devrait être limitée; il y a donc lieu de prévoir des garanties [...] appropriées. Dans le cas d'enfants, ces signalements et les procédures correspondantes devraient servir l'intérêt supérieur de l'enfant, compte tenu de l'article 24 de la charte des droits fondamentaux de l'Union européenne et de la convention des Nations unies relative aux droits de l'enfant du 20 novembre 1989.

(23 bis) Les signalements d'enfants risquant d'être enlevés devraient être introduits dans le SIS à la demande des autorités compétentes, y compris les autorités judiciaires compétentes en matière de responsabilité parentale conformément au droit national.

¹⁵ Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

(23 ter) Les signalements de personnes vulnérables qui doivent être empêchées de voyager pour leur propre protection devraient être introduits par exemple lorsqu'il y a lieu de croire que le voyage entraînerait un risque de mariage forcé, de mutilation sexuelle féminine, de traite d'êtres humains ou, dans le cas d'enfants, d'enrôlement dans des conflits armés, des organisations criminelles ou des groupes terroristes.

(24) Une nouvelle conduite à tenir devrait être ajoutée pour les soupçons liés au terrorisme et aux infractions graves, qui permettrait [...] d'interroger une personne soupçonnée d'avoir commis une infraction grave ou lorsqu'il existe des raisons de croire qu'elle va commettre une telle infraction [...], **sous réserve du droit national**, afin de fournir les informations les plus détaillées possibles à l'État membre signalant. Cette nouvelle conduite **à tenir lors du contrôle de police ou des vérifications aux frontières** ne devrait pas revenir à fouiller la personne ni à l'arrêter, **et les droits procéduraux de la personne devraient être préservés. Elle s'entend en outre sans préjudice des mécanismes d'entraide judiciaire existants.** Elle devrait cependant permettre d'obtenir suffisamment d'informations pour que **les autorités signalantes et les autorités d'exécution** décident **entre elles** des mesures à prendre **en temps réel dans toute la mesure du possible.** Les "infractions graves" devraient correspondre aux infractions énumérées dans la décision-cadre 2002/584/JAI du Conseil.

(24 bis) En cas de signalements d'objets aux fins d'une saisie ou de la preuve dans une procédure pénale, les objets devraient en principe être saisis. Cependant, le droit national détermine si un objet est saisi et dans quelles conditions, en particulier s'il est en la possession de son propriétaire légitime.

(25) Le SIS devrait comporter de nouvelles catégories d'objets de grande valeur, tels que les **produits informatiques** [...], qui peuvent être identifiés et faire l'objet d'une consultation avec un numéro unique.

(25 bis) En ce qui concerne les documents à insérer aux fins d'une saisie ou de la preuve dans une procédure pénale, le terme "faux" devrait s'entendre comme désignant aussi bien les documents falsifiés que les documents contrefaits.

- (26) Il y a lieu de prévoir la possibilité pour un État membre d'apposer sur le signalement une mention, appelée "indicateur de validité", tendant à ce que la conduite à tenir qui est demandée dans le signalement ne soit pas exécutée sur son territoire. Lorsque des signalements sont introduits en vue d'une arrestation aux fins de remise, rien dans le présent **règlement** [...] ne devrait être interprété comme dérogeant aux dispositions de la décision-cadre 2002/584/JAI ou comme en empêchant l'application. La décision d'apposer un indicateur de validité sur un signalement **en vue de la non-exécution d'un mandat d'arrêt européen** ne devrait être fondée que sur les motifs de refus prévus dans ladite décision-cadre.
- (27) Lorsqu'un indicateur de validité a été apposé et que le lieu où se trouve la personne recherchée en vue d'une arrestation aux fins de remise vient à être connu, ce lieu devrait toujours être communiqué à l'autorité judiciaire d'émission, qui peut décider de transmettre un mandat d'arrêt européen à l'autorité judiciaire compétente conformément aux dispositions de la décision-cadre 2002/584/JAI.
- (28) Il devrait être possible pour les États membres de mettre en relation les signalements dans le SIS. Cette mise en relation par un État membre de deux ou plusieurs signalements ne devrait avoir aucun effet sur la conduite à tenir, la durée de conservation ou les droits d'accès aux signalements.

(29) Les signalements ne devraient pas être conservés dans le SIS pour une durée plus longue que le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits. Afin de réduire la charge administrative des différentes autorités qui traiteront des données relatives aux personnes pour différentes finalités, il y a lieu d'aligner la durée de conservation des signalements de personnes sur les durées de conservation envisagées pour le retour et pour le séjour irrégulier. De plus, les États membres prorogent régulièrement la date d'expiration des signalements de personnes si la conduite à tenir n'a pas pu être exécutée dans le délai initial. En conséquence, la durée de conservation des signalements de personnes devrait être de cinq ans au maximum. À titre de principe général, les signalements de personnes devraient être automatiquement supprimés du SIS après cinq ans, sauf ceux introduits aux fins de contrôle discret, de contrôle spécifique et de contrôle d'investigation, qui devraient être supprimés après un an. Les signalements d'objets [...] devraient être automatiquement supprimés du SIS après **dix** [...] ans car, au terme de ce délai, la probabilité de les retrouver est très faible et leur valeur économique a considérablement diminué. Les signalements **d'objets, lorsqu'ils sont liés à des signalements de personnes** [...], **ne** devraient **pas** être conservés **plus longtemps que les signalements de personnes auxquels ils sont liés et, en tout état de cause, ils ne devraient pas être conservés pendant plus de cinq** ans [...]. La décision de conserver des signalements de personnes devrait être fondée sur une évaluation individuelle complète. Les États membres devraient réexaminer les signalements de personnes **et d'objets** [...] **à intervalles réguliers** [...] et tenir des statistiques concernant le nombre de signalements [...] dont la durée de conservation a été prolongée.

- (30) Lors de l'introduction et de la prorogation de la date d'expiration d'un signalement dans le SIS, il convient de respecter l'exigence de proportionnalité, en vérifiant si un cas déterminé est suffisamment approprié, pertinent et important pour justifier l'introduction d'un signalement dans le SIS. Les infractions décrites aux articles **3 à 14 de la directive (UE) 2017/541**¹⁶ [...] ¹⁷ constituent des menaces très graves contre la sécurité publique et l'intégrité des personnes et contre la société, et il est extrêmement difficile de les prévenir et de les détecter ainsi que d'enquêter à leur sujet dans un espace sans contrôles aux frontières intérieures, où les malfaiteurs potentiels circulent librement. Si une personne ou un objet est recherché en rapport avec ces infractions, il est [...] nécessaire de créer dans le SIS le signalement correspondant des personnes recherchées aux fins d'une procédure judiciaire pénale, des personnes ou objets soumis à un contrôle discret, d'investigation ou spécifique, ainsi que des objets recherchés aux fins d'une saisie, car aucun autre moyen ne sera aussi efficace à cet effet. **À titre exceptionnel, les États membres peuvent s'abstenir de créer le signalement si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires liées à la sécurité publique ou nationale.**
- (31) Il est nécessaire d'apporter des éclaircissements sur la suppression des signalements. Un signalement ne devrait être conservé que pendant la durée nécessaire à la réalisation de la finalité pour laquelle il a été introduit. Compte tenu des pratiques divergentes des États membres en ce qui concerne la définition du moment où un signalement a atteint son objectif, il convient d'établir pour chaque catégorie de signalements des critères détaillés permettant de déterminer quand le signalement devrait être supprimé du SIS.
- (32) L'intégrité des données du SIS est de la plus haute importance. Il convient dès lors de prévoir des mesures de protection adaptées pour que les données du SIS soient traitées, au niveau tant central que national, d'une manière qui assure leur sécurité de bout en bout. Les autorités intervenant dans le traitement des données devraient être liées par les obligations de sécurité imposées par le présent règlement et soumises à une procédure uniforme de déclaration des incidents.

¹⁶ Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

¹⁷ [...]

(33) Les données traitées dans le SIS en application du présent règlement ne devraient pas être transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition.
[...]

(34) Il y a lieu d'accorder un accès au SIS aux autorités chargées d'immatriculer les véhicules, les bateaux et les aéronefs pour leur permettre de vérifier si le moyen de transport est déjà recherché dans un autre État membre aux fins de saisie ou de contrôle. [...] ¹⁸ [...] ¹⁹

(34 bis) Il y a lieu d'accorder un accès au SIS aux autorités chargées d'enregistrer les armes à feu pour leur permettre de vérifier si l'arme à feu est déjà recherchée dans un autre État membre aux fins de saisie ou de contrôle ou s'il existe un signalement concernant la personne qui demande l'enregistrement.

¹⁸ [...]

¹⁹ Déplacé vers le considérant 34 *ter*.

(34 ter)²⁰ Un accès direct devrait être octroyé aux autorités compétentes qui sont des services publics. Cet accès devrait être limité aux signalements concernant les moyens de transport en cause et leur document ou plaque d'immatriculation, ou les armes à feu en cause et les personnes demandant leur enregistrement. En conséquence, il convient d'intégrer dans le présent règlement les dispositions du règlement (CE) n° 1986/2006 du Parlement européen et du Conseil²¹ et d'abroger ledit règlement. Toute réponse positive dans le SIS doit être signalée par les autorités susmentionnées aux services de police aux fins de procédures complémentaires conformément au signalement particulier figurant dans le SIS et aux fins de la notification de la réponse positive à l'État membre signalant par l'intermédiaire des bureaux SIRENE.

- (35) Les dispositions nationales transposant la directive (UE) 2016/680 devraient s'appliquer aux traitements de données effectués par les autorités nationales compétentes à des fins de prévention et de détection d'infractions graves ou terroristes, d'enquêtes en la matière, de poursuites en cas d'infractions pénales et d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Il convient, lorsque c'est nécessaire, de préciser davantage dans le présent règlement les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil²² et de la directive (UE) 2016/680.
- (36) Le règlement (UE) 2016/679 devrait s'appliquer aux traitements de données à caractère personnel effectués en vertu du présent règlement par les autorités nationales lorsque la directive (UE) 2016/680 ne s'applique pas. Le règlement (CE) n° 45/2001 du Parlement européen et du Conseil²³ devrait s'appliquer aux traitements de données à caractère personnel effectués par les institutions et organes de l'Union dans l'exercice de leurs fonctions en vertu du présent règlement.

²⁰ Texte déplacé en partie depuis le considérant 34.

²¹ Règlement (CE) n° 1986/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28.12.2006, p. 1).

²² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

²³ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

- (37) Il convient, lorsque c'est nécessaire, de préciser davantage dans le présent règlement les dispositions de la directive (UE) 2016/680, du règlement (UE) 2016/679 et du règlement (CE) n° 45/2001. En ce qui concerne le traitement de données à caractère personnel par Europol, le règlement (UE) 2016/794 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (règlement Europol)²⁴ est applicable.
- En ce qui concerne le traitement de données à caractère personnel par Eurojust, la décision 2002/187/JAI est applicable.**
- (38) Les dispositions en matière de protection des données contenues dans la décision 2002/187/JAI du 28 février 2002²⁵ instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité s'appliquent au traitement des données du SIS par Eurojust, notamment celles concernant le pouvoir qu'a l'organe de contrôle commun, créé par cette décision, de contrôler les activités d'Eurojust et celles concernant la responsabilité découlant de tout traitement non autorisé de données à caractère personnel effectué par Eurojust. Lorsqu'il ressort d'une consultation du SIS par Eurojust qu'il existe un signalement introduit par un État membre, Eurojust ne peut pas exécuter la conduite à tenir requise. Il devrait dès lors informer l'État membre concerné pour lui permettre de donner suite à l'affaire.
- (39) En ce qui concerne la confidentialité, les dispositions pertinentes du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne devraient s'appliquer aux fonctionnaires et autres agents employés et travaillant en liaison avec le SIS.
- (40) Tant les États membres que l'agence eu-LISA devraient disposer de plans de sécurité visant à faciliter la mise en œuvre des obligations en matière de sécurité, ainsi que coopérer de manière à traiter les questions de sécurité dans une perspective commune.
- (41) Les autorités de contrôle indépendantes nationales devraient vérifier la licéité des traitements de données à caractère personnel effectués par les États membres dans le cadre du présent règlement. Le droit des personnes concernées d'avoir accès à leurs données à caractère personnel stockées dans le SIS et d'en obtenir la rectification et l'effacement, ainsi que les recours juridictionnels ultérieurs et la reconnaissance mutuelle des décisions judiciaires, devraient être précisés. Il y a donc lieu d'imposer aux États membres de communiquer des statistiques annuelles.

²⁴ Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

²⁵ Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité (JO L 63 du 6.3.2002, p. 1).

- (42) Les autorités de contrôle devraient veiller à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans **leur** [...] N.SIS, répondant aux normes internationales en matière d'audit. Cet audit devrait être réalisé par les autorités de contrôle elles-mêmes ou être commandé directement par elles à un auditeur indépendant en matière de protection des données. Ce dernier devrait rester sous le contrôle et la responsabilité de la ou des autorités de contrôle nationales, qui devraient donc commander l'audit proprement dit et définir clairement son objet, son étendue et sa méthode, et donner des indications et des instructions sur l'audit et ses résultats finaux.
- (43) Le règlement (UE) 2016/794 (règlement Europol) prévoit qu'Europol soutient et renforce l'action des autorités compétentes des États membres et leur coopération mutuelle dans la prévention du terrorisme et des formes graves de criminalité et qu'il fournit des analyses et des évaluations de la menace. L'élargissement du droit d'accès d'Europol aux signalements du SIS concernant des personnes disparues devrait accroître encore sa capacité d'apporter aux autorités répressives nationales un appui opérationnel et analytique complet en matière de traite des êtres humains et d'exploitation sexuelle des enfants, y compris en ligne. Europol contribuerait ainsi à une meilleure prévention de ces infractions pénales, à la protection des victimes potentielles et aux enquêtes sur les auteurs de ces infractions. Ce nouveau droit d'accès d'Europol aux signalements du SIS concernant des personnes disparues bénéficierait aussi à son Centre européen de lutte contre la cybercriminalité, notamment pour les cas de tourisme sexuel et de pédopornographie en ligne, où les délinquants affirment souvent avoir accès, ou pouvoir avoir accès, à des enfants qui sont susceptibles d'avoir été enregistrés comme personnes disparues. [...]

- (44) 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 [...] **peuvent** partager avec Europol leurs informations sur les activités liées au terrorisme **lors de** [...] l'introduction de signalements dans le SIS, ainsi que les réponses positives et les informations y afférentes. **Ce partage d'informations devrait s'effectuer par voie d'échange d'informations supplémentaires avec Europol sur les signalements correspondants. À cette fin, Europol devrait établir une connexion avec l'infrastructure de communication du réseau SIRENE.** Le Centre européen de lutte contre le terrorisme, créé au sein d'Europol, pourrait ainsi vérifier s'il existe des informations contextuelles supplémentaires dans les bases de données d'Europol et produire des analyses de grande qualité qui aideraient à démanteler les réseaux terroristes et, si possible, à les empêcher de commettre des attentats.
- (45) Il est également nécessaire d'établir des règles précises au sujet du traitement et du téléchargement par Europol des données du SIS, pour permettre l'utilisation la plus complète du système, à condition que les normes de protection des données soient respectées comme le prévoient le présent règlement et le règlement (UE) 2016/794. Lorsqu'il ressort d'une consultation du SIS par Europol qu'il existe un signalement introduit par un État membre, Europol ne peut pas exécuter la conduite à tenir requise. Il devrait dès lors informer l'État membre concerné **par voie d'échange d'informations supplémentaires avec le bureau SIRENE concerné** pour lui permettre de donner suite à l'affaire.

(46) Le règlement (UE) 2016/1624 du Parlement européen et du Conseil²⁶ prévoit, aux fins dudit règlement, que l'État membre hôte autorise les membres des équipes du corps européen de garde-frontières et de garde-côtes ou d'équipes d'agents intervenant dans les tâches liées aux retours, déployées par l'Agence européenne de garde-frontières et de garde-côtes, à consulter les bases de données européennes, lorsque cette consultation est nécessaire à la réalisation des objectifs opérationnels spécifiés dans le plan opérationnel relatif aux vérifications aux frontières, à la surveillance des frontières et au retour. D'autres agences concernées de l'Union, en particulier le Bureau européen d'appui en matière d'asile et Europol, peuvent également déployer, dans le cadre des équipes d'appui à la gestion des flux migratoires, des experts qui n'appartiennent pas au personnel de ces agences de l'Union. Le déploiement d'équipes du corps européen de garde-frontières et de garde-côtes, d'équipes d'agents intervenant dans les tâches liées aux retours et d'équipes d'appui à la gestion des flux migratoires a pour objectif de fournir des renforts techniques et opérationnels aux États membres demandeurs, en particulier à ceux confrontés à des défis migratoires disproportionnés. Pour accomplir les tâches qui leur sont confiées, ces différentes équipes ont besoin d'avoir accès au SIS grâce à une interface technique de l'Agence européenne de garde-frontières et de garde-côtes qui permette de se connecter au SIS central. Lorsqu'il ressort d'une consultation du SIS par l'équipe ou les équipes d'agents qu'il existe un signalement introduit par un État membre, le membre de l'équipe ou l'agent ne peut exécuter la conduite à tenir requise que si l'État membre hôte l'y autorise. Il devrait dès lors informer l'État membre **hôte** [...] pour lui permettre de donner suite à l'affaire. **L'État membre hôte devrait notifier la réponse positive à l'État membre signalant par voie d'échange d'informations supplémentaires.**

²⁶ Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) n° 863/2007 du Parlement européen et du Conseil, le règlement (CE) n° 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

- (47) Conformément à la proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)²⁷, présentée par la Commission, l'unité centrale ETIAS de l'Agence européenne de garde-frontières et de garde-côtes effectuera des vérifications dans le SIS via l'ETIAS pour réaliser l'évaluation des demandes d'autorisation de voyage, qui requiert notamment de vérifier si le ressortissant de pays tiers qui demande une autorisation de voyage fait l'objet d'un signalement dans le SIS. À cette fin, l'unité centrale ETIAS au sein de l'Agence européenne de garde-frontières et de garde-côtes devrait également avoir accès au SIS dans la mesure nécessaire à l'accomplissement de sa mission, c'est-à-dire à toutes les catégories de signalements de personnes et aux signalements de documents personnels d'identité vierges et délivrés.
- (48) En raison de leur nature technique, de leur niveau de précision et de la nécessité de les actualiser à intervalles réguliers, certains aspects du SIS ne peuvent pas être couverts de manière exhaustive par les dispositions du présent règlement. Il s'agit, par exemple, des règles techniques concernant l'introduction, l'actualisation, la suppression et la consultation des données, de la qualité des données et des règles de consultation liées aux **données** [...] biométriques, des règles de compatibilité et de priorité entre les signalements, [...] de la mise en relation des signalements, de l'indication de nouvelles catégories d'objets dans la catégorie des équipements techniques et électroniques, de la fixation de la date d'expiration des signalements dans les limites du délai maximal et de l'échange d'informations supplémentaires. Les compétences d'exécution relatives à ces aspects devraient par conséquent être conférées à la Commission. Les règles techniques concernant les consultations de signalements devraient tenir compte du bon fonctionnement des applications nationales.
- (49) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec **l'article 5 du** règlement (UE) n° 182/2011²⁸. La procédure d'adoption des mesures d'application à arrêter en vertu du présent règlement et du règlement (UE) 2018/xxx (sur les vérifications aux frontières) devrait être identique.

²⁷ COM (2016)731 final.

²⁸ Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

- (50) Pour assurer la transparence, l'agence eu-LISA devrait présenter tous les deux ans un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité offerte, et sur les échanges **bilatéraux et multilatéraux** d'informations supplémentaires. La Commission devrait procéder à une évaluation globale tous les quatre ans.
- (51) Étant donné que les objectifs du présent règlement, à savoir l'établissement d'un système d'information commun et la fixation de règles applicables à ce dernier ainsi que l'échange d'informations supplémentaires, ne peuvent pas, de par leur nature même, être réalisés de manière suffisante par les États membres et peuvent donc être mieux réalisés au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'il est énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.
- (52) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus, notamment, par la charte des droits fondamentaux de l'Union européenne. En particulier, il cherche à assurer un environnement sûr à toutes les personnes résidant sur le territoire de l'Union européenne et une protection spéciale aux enfants qui risquent d'être victimes de la traite des êtres humains ou d'un enlèvement parental, tout en respectant pleinement la protection des données à caractère personnel.
- (53) Conformément aux articles 1^{er} et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application. Le présent règlement développant l'acquis de Schengen, le Danemark décide, conformément à l'article 4 dudit protocole, dans un délai de six mois à partir de la décision du Conseil sur le présent règlement, s'il le transpose dans son droit national.

- (54) Le Royaume-Uni participe au présent règlement, conformément à l'article 5, **paragraphe 1**, du protocole **n° 19** sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et conformément à l'article 8, paragraphe 2, de la décision 2000/365/CE du Conseil [...] ²⁹.
- (55) L'Irlande participe au présent règlement, conformément à l'article 5 [...] du protocole **n° 19** sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et conformément à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil [...] ³⁰.
- (56) En ce qui concerne l'Islande et la Norvège, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ³¹, qui relèvent du domaine visé à l'article 1^{er}, point G, de la décision 1999/437/CE du Conseil ³² relative à certaines modalités d'application de cet accord.

²⁹ [...]

³⁰ [...]

³¹ JO L 176 du 10.7.1999, p. 36.

³² JO L 176 du 10.7.1999, p. 31.

(57) En ce qui concerne la Suisse, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord [...] entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen qui relèvent du domaine visé à l'article 1^{er}, point G, de la décision 1999/437/CE, lu en liaison avec l'article **3** [...] de la [...] ³³ [...] ³⁴ [...] décision **2008/149/JAI** du Conseil³⁵.

³³ [...]

³⁴ [...]

³⁵ Décision 2008/149/JAI du Conseil du 28 janvier 2008 relative à la conclusion, au nom de l'Union européenne, de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 53 du 27.2.2008, p. 50).

- (58) En ce qui concerne le Liechtenstein, le présent règlement constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen³⁶ qui relèvent du domaine visé à l'article 1^{er}, point G, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2011/349/UE du Conseil³⁷ [...] ³⁸.
- (59) En ce qui concerne la Bulgarie, [...] la Roumanie **et la Croatie**, le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens, **respectivement**, de l'article 4, paragraphe 2, de l'acte d'adhésion de 2005 **et de l'article 4, paragraphe 2, de l'acte d'adhésion de 2011**, et il doit être lu en combinaison avec, **respectivement**, la décision 2010/365/UE du Conseil sur l'application à la République de Bulgarie et à la Roumanie des dispositions de l'acquis de Schengen relatives au système d'information Schengen³⁹ **et la décision 2017/733 du Conseil sur l'application en République de Croatie des dispositions de l'acquis de Schengen relatives au système d'information Schengen**⁴⁰.

³⁶ JO L 160 du 18.6.2011, p. 3.

³⁷ Décision 2011/349/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen notamment en ce qui concerne la coopération judiciaire en matière pénale et la coopération policière (JO L 160 du 18.6.2011, p. 1).

³⁸ [...]

³⁹ JO L 166 du 1.7.2010, p. 17.

⁴⁰ JO L 108 du 26.4.2017, p. 31.

- (60) En ce qui concerne Chypre [...], le présent règlement constitue un acte fondé sur l'acquis de Schengen ou qui s'y rapporte, au sens [...] de l'article 3, paragraphe 2, de l'acte d'adhésion de 2003 [...].
- (61) Le présent règlement devrait s'appliquer à l'Irlande à des dates fixées conformément aux procédures prévues dans les instruments pertinents concernant l'application de l'acquis de Schengen à cet État.
- (62) [...] ⁴¹ [...]
- (63) La décision 2007/533/JAI du Conseil et la décision 2010/261/UE ⁴² de la Commission devraient dès lors être abrogées.
- (64) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, et a rendu son avis le [...],

⁴¹ [...]

⁴² Décision 2010/261/UE de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication (JO L 112 du 5.5.2010, p. 31).

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objectif général du SIS

L'objet du SIS est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que **d'assurer l'application des** dispositions de la troisième partie, titre V, chapitres 4 et 5, du traité sur le fonctionnement de l'Union européenne relatives à la libre circulation des personnes sur les territoires des États membres, à l'aide des informations transmises par ce système.

Article 2

Champ d'application

1. Le présent règlement établit les conditions et les procédures relatives à l'introduction et au traitement dans le SIS des signalements de personnes ou d'objets, ainsi qu'à l'échange d'informations supplémentaires et de données complémentaires aux fins de la coopération policière et de la coopération judiciaire en matière pénale.
2. Le présent règlement contient également des dispositions concernant l'architecture technique du SIS et les responsabilités incombant aux États membres et à 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, des règles générales sur le traitement des données, ainsi que des dispositions sur les droits des personnes concernées et sur la responsabilité.

Article 3
Définitions

1. Aux fins du présent règlement, on entend par:
 - a) "signalement", un ensemble de données, y compris, **le cas échéant**, les **données** [...] biométriques mentionnées aux articles 22 et 40, introduites dans le SIS pour permettre aux autorités compétentes d'identifier une personne ou un objet en vue de tenir une conduite particulière à son égard;
 - b) "informations supplémentaires", les informations ne faisant pas partie des données d'un signalement stockées dans le SIS, mais en rapport avec des signalements introduits dans le SIS, qui doivent être échangées **par l'intermédiaire des bureaux SIRENE**:
 - 1) afin de permettre aux États membres de se consulter ou de s'informer mutuellement lors de l'introduction d'un signalement;
 - 2) à la suite d'une réponse positive afin que la conduite à tenir demandée puisse être exécutée;
 - 3) en cas d'impossibilité d'exécuter la conduite à tenir demandée;
 - 4) en ce qui concerne la qualité des données du SIS;
 - 5) en ce qui concerne la compatibilité et la priorité entre les signalements;
 - 6) en ce qui concerne l'exercice du droit d'accès;
 - c) "données complémentaires", les données stockées dans le SIS et en rapport avec des signalements introduits dans le SIS, qui doivent être immédiatement accessibles aux autorités compétentes lorsqu'une personne au sujet de laquelle des données ont été introduites dans le SIS est localisée à la suite de consultations effectuées dans ce système;
 - d) "données à caractère personnel", toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée");

- e) "personne physique identifiable", une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;
- f) "traitement de données à caractère personnel", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement dans un journal, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;
- g) "[...] **correspondance**" [...], **la succession des étapes suivantes:**
- 1) une consultation est effectuée par un utilisateur **final**,
 - 2) il ressort de la consultation qu'il existe un signalement introduit par un autre État membre dans le SIS, **et**
 - 3) les données relatives au signalement introduit dans le SIS correspondent aux données de la consultation; [...]

g bis) "réponse positive", une correspondance qui satisfait aux critères suivants:

a) elle a été confirmée:

i) par l'utilisateur final, ou

ii) si la correspondance en question est fondée sur la comparaison de données biométriques, par l'autorité compétente conformément aux procédures nationales;

et

[...] **b)** une conduite à tenir est demandée;

- h) "indicateur de validité", une suspension de la validité d'un signalement au niveau national, qui peut être ajoutée aux signalements en vue d'une arrestation, aux signalements de personnes disparues **et vulnérables** et aux signalements aux fins de contrôle discret, de contrôle d'investigation ou de contrôle spécifique [...];
- i) "État membre signalant", l'État membre qui introduit le signalement dans le SIS;
- j) "État membre d'exécution", l'État membre qui exécute ou a exécuté la conduite à tenir à la suite d'une réponse positive;
- k) "utilisateurs finaux", les autorités compétentes qui consultent directement le CS-SIS, le N.SIS ou une copie technique de ceux-ci;

k bis) "données biométriques", les données biométriques au sens de l'article 3, point 13, de la directive (UE) 2016/680;

- l) "données dactylo[...]scopiques", [...] **les images d'**empreintes digitales, **images d'empreintes digitales latentes** [...], d'empreintes de paumes de mains, **d'empreintes de paumes de mains latentes, ainsi que des modèles de telles images (points caractéristiques codés)**⁴³, qui, en raison de leur caractère unique et des points de référence qu'elles contiennent, permettent de réaliser des comparaisons précises et concluantes en ce qui concerne l'identité d'une personne;

l bis) "image faciale", les images numériques du visage de la personne, d'une résolution et d'une qualité d'image suffisantes pour servir à l'établissement automatisé de correspondances biométriques⁴⁴;

l ter) "profil ADN", un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci)⁴⁵;

⁴³ Définition identique à celle figurant dans la décision 2008/616/JAI du Conseil.

⁴⁴ Définition identique à celle figurant dans la proposition relative à l'EES (voir l'article 3, point 16), dans le doc. 11037/17 + ADD 1 + ADD 2).

⁴⁵ Définition identique à celle figurant à l'article 2, point c), de la décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 12).

- m) "infractions graves", les infractions énumérées à l'article 2, paragraphes 1 et 2, de la décision-cadre 2002/584/JAI du 13 juin 2002⁴⁶;
- n) "infraction terroriste", [...] **une** infraction prévue par le droit national **qui correspond ou est équivalente à l'une des infractions** visées [...] par la [...] ⁴⁷ **directive (UE) 2017/541**⁴⁸;
- o) "personnes vulnérables", les personnes qui, en raison de leur âge, de leur état physique ou mental ou de leur situation sociale ou familiale, ont besoin d'une protection;**
- p) "menace pour la santé publique", une menace pour la santé publique au sens du règlement (UE) 2016/399**⁴⁹.

Article 4

Architecture technique et mode de fonctionnement du SIS

1. Le SIS se compose:
 - a) d'un système central (ci-après dénommé "SIS central") comprenant:
 - une fonction de support technique (ci-après dénommée "CS-SIS") contenant la base de données du SIS;
 - une interface nationale uniforme (ci-après dénommée "NI-SIS");

⁴⁶ Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

⁴⁷ [...]

⁴⁸ Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

⁴⁹ Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen).

b) d'une section nationale (ci-après dénommée "N.SIS") dans chaque État membre, constituée des systèmes de données nationaux reliés au SIS central. Un N.SIS [...] **peut contenir** un fichier de données (ci-après dénommé "copie nationale") comportant une copie complète ou partielle de la base de données du SIS [...]. **Deux ou plusieurs États membres peuvent établir dans l'un de leurs N.SIS nationaux une copie partagée qui peut être utilisée conjointement par ces États membres. Cette copie partagée est considérée comme la copie nationale de chacun des États membres participants;**

b bis) d'au moins un site de secours national ou partagé dans chaque N.SIS. Un N.SIS de secours partagé peut être utilisé conjointement par deux ou plusieurs États membres et est considéré comme le N.SIS de secours de chacun des États membres participants. Le N.SIS et sa version de secours peuvent être utilisés simultanément en vue d'assurer la disponibilité continue pour les utilisateurs finaux; **et**

c) d'une infrastructure de communication entre le CS-SIS et le NI-SIS (ci-après dénommée "infrastructure de communication"), fournissant un réseau virtuel crypté consacré aux données du SIS et à l'échange de données entre les bureaux SIRENE visés à l'article 7, paragraphe 2.

2. [...] **Les États membres** [...] **introduisent**, mettent à jour, suppriment et consultent **les données du SIS** par l'intermédiaire des différents N.SIS. Une copie nationale **ou partagée** partielle ou complète est disponible pour effectuer des consultations automatisées sur le territoire de chacun des États membres utilisant une telle copie. La copie nationale **ou partagée** partielle contient au moins les données mentionnées à l'article 20, paragraphe 2, en ce qui concerne les objets, et les données énumérées à l'article 20, paragraphe 3, points a) à v) **et point z)**, du présent règlement en ce qui concerne les signalements de personnes. Il n'est pas possible de consulter les fichiers de données des N.SIS des autres États membres.

3. Le CS-SIS assure des fonctions techniques de contrôle et de gestion et dispose d'un CS-SIS de secours capable d'assurer l'ensemble des fonctionnalités du CS-SIS principal en cas de défaillance de celui-ci. **Le CS-SIS et sa version de secours peuvent fonctionner simultanément.** Le CS-SIS et sa version de secours sont 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, créée par le règlement (UE) n °1077/2011 (ci-après dénommée "agence eu-LISA"). Le CS-SIS ou sa version de secours peuvent contenir une copie [...] **technique** de la base de données du SIS [...] **qui peut** être utilisée simultanément [...], à condition que chacun d'eux soit capable de traiter toutes les transactions liées aux signalements introduits dans le SIS.
4. Le CS-SIS assure les services nécessaires à l'introduction et au traitement des données du SIS, y compris les consultations dans la base de données du SIS. Le CS-SIS assure:
 - a) la mise à jour en ligne de la copie nationale;
 - b) la synchronisation et la cohérence entre la copie nationale et la base de données du SIS;
 - c) les opérations d'initialisation et de restauration de la copie nationale; **et**
 - d) la disponibilité continue.

Article 5

Coûts

1. Les coûts d'exploitation, de maintenance et de développement ultérieur du SIS central et de l'infrastructure de communication sont à la charge du budget général de l'Union européenne.
2. Ces coûts couvrent les travaux effectués en ce qui concerne le CS-SIS afin d'assurer la fourniture des services visés à l'article 4, paragraphe 4.
3. Les coûts de mise en place, d'exploitation, de maintenance et de développement ultérieur de chaque N.SIS sont à la charge de l'État membre concerné.

CHAPITRE II

RESPONSABILITÉS INCOMBANT AUX ÉTATS MEMBRES

Article 6

Systèmes nationaux

Chaque État membre est chargé de mettre en place, d'exploiter et de continuer à développer son N.SIS, ainsi que d'en assurer la maintenance, et de le connecter au NI-SIS.

Chaque État membre est chargé d'assurer le fonctionnement continu du N.SIS, sa connexion au NI-SIS et la disponibilité continue des données du SIS pour les utilisateurs finaux.

Chaque État membre transmet ses signalements par l'intermédiaire de son N.SIS⁵⁰.

Article 7

Office N.SIS et bureau SIRENE

1. Chaque État membre désigne une autorité (ci-après dénommée "office N.SIS") qui assume la responsabilité centrale du N.SIS.

Cette autorité est responsable du bon fonctionnement et de la sécurité du N.SIS, fait en sorte que les autorités compétentes aient accès au SIS et prend les mesures nécessaires pour assurer le respect des dispositions du présent règlement. Elle est chargée de veiller à ce que toutes les fonctionnalités du SIS soient dûment mises à la disposition des utilisateurs finaux.

[...] ⁵¹

⁵⁰ Déplacé depuis l'article 7, paragraphe 1, in fine, exception faite du terme "office" avant "N.SIS".

⁵¹ Déplacé vers l'article 6 in fine.

2. Chaque État membre désigne l'autorité chargée d'assurer l'échange et la disponibilité de toutes les informations supplémentaires (ci-après dénommée "bureau SIRENE"), conformément aux dispositions du manuel SIRENE, tel qu'il est visé à l'article 8.

Ces bureaux coordonnent également la vérification de la qualité des informations introduites dans le SIS. À ces fins, ils ont accès aux données traitées dans le SIS.

3. Les États membres communiquent à l'agence eu-LISA les coordonnées de leur office N.SIS et de leur bureau SIRENE. L'agence eu-LISA publie la liste de ces coordonnées ainsi que celle visée à l'article 53, paragraphe 8.

Article 8

Échange d'informations supplémentaires

1. Les informations supplémentaires sont échangées conformément aux dispositions du manuel SIRENE, au moyen de l'infrastructure de communication. Les États membres fournissent les moyens techniques et humains nécessaires pour assurer la disponibilité permanente et l'échange d'informations supplémentaires. Au cas où l'infrastructure de communication ne serait pas accessible, les États membres peuvent utiliser d'autres moyens techniques correctement sécurisés pour échanger des informations supplémentaires.
2. Les informations supplémentaires sont utilisées exclusivement aux fins auxquelles elles ont été transmises, conformément à l'article 61, sauf accord préalable de l'État membre signalant.
3. Les bureaux SIRENE s'acquittent de leur tâche de manière rapide et efficace, notamment en [...] **réagissant** aux demandes dans les meilleurs délais, **mais de préférence** au plus tard 12 heures après leur réception.

4. **La Commission adopte des actes d'exécution pour établir les** modalités relatives à l'échange d'informations supplémentaires **sous la forme d'un manuel intitulé "manuel SIRENE". Ces actes d'exécution** sont adoptés [...] en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2 [...].

Article 9

Conformité technique et fonctionnelle

1. Pour permettre une transmission rapide et efficace des données, chaque État membre applique, lors de la création de son N.SIS, les normes communes, les protocoles et les procédures techniques établis afin de permettre la compatibilité de son N.SIS avec le CS-SIS. [...] ⁵²
2. Les États membres veillent, au moyen des services fournis par le CS-SIS et des mises à jour automatiques visées à l'article 4, paragraphe 4, à ce que les données stockées dans la copie nationale **ou partagée** soient identiques à celles de la base de données du SIS et compatibles avec elles, et à ce qu'une consultation de cette copie produise un résultat équivalent à celui d'une consultation dans la base de données du SIS. Les utilisateurs finaux reçoivent les données dont ils ont besoin pour s'acquitter de leurs tâches, en particulier toutes les données nécessaires pour identifier la personne concernée et exécuter la conduite à tenir demandée.

- 3.⁵³ La Commission adopte des actes d'exécution pour établir et préciser les normes communes, les protocoles et les procédures techniques visés au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.**

⁵² Déplacé vers le paragraphe 3.

⁵³ Déplacé depuis le paragraphe 1 in fine.

Article 10
Sécurité - États membres

1. Chaque État membre adopte, pour son N.SIS, les mesures, dont un plan de sécurité, un plan de continuité des opérations et un plan de rétablissement après sinistre, propres à:
 - a) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;
 - b) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès aux installations);
 - c) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);
 - d) empêcher l'introduction non autorisée de données ainsi que tout examen, toute modification ou tout effacement non autorisés de données à caractère personnel stockées (contrôle du stockage);
 - e) empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);
 - f) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des [...] **identificateurs**⁵⁴ d'utilisateur individuels et uniques ainsi qu'à des modes d'accès confidentiels (contrôle de l'accès aux données);

⁵⁴ Libellé identique à celui de l'article 12, paragraphes 2 et 3, et de l'article 18, paragraphes 2 et 3.

- g) garantir que toutes les autorités ayant un droit d'accès au SIS ou aux installations de traitement de données créent des profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées en matière d'accès, d'introduction, de mise à jour, de suppression et de consultation des données et mettent sans tarder et à leur demande ces profils à la disposition des autorités de contrôle nationales visées à l'article [...] **67** (profils des membres du personnel);
 - h) garantir qu'il puisse être vérifié et constaté à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);
 - i) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment, par qui et à quelle fin (contrôle de l'introduction);
 - j) empêcher, en particulier par des techniques de cryptage adaptées, que, lors de la transmission de données à caractère personnel ou du transport de support de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport); **et**
 - k) contrôler l'efficacité des mesures de sécurité prévues au présent paragraphe et prendre les mesures organisationnelles nécessaires en matière de contrôle interne (autosurveillance).
2. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement et des échanges d'informations supplémentaires, y compris la sécurisation des locaux du bureau SIRENE.
3. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement des données du SIS effectué par les autorités mentionnées à l'article 43.
- 4. Les mesures décrites aux paragraphes 1 à 3 peuvent faire partie d'une approche et d'un plan de sécurité génériques au niveau national. Les exigences du présent article et son applicabilité au SIS sont toutefois clairement identifiables et respectées dans ce plan.**

Article 11
Confidentialité - États membres

Chaque État membre applique à l'égard de toutes les personnes et de tous les organismes appelés à travailler avec des données du SIS et des informations supplémentaires ses règles relatives au secret professionnel ou leur impose des obligations de confidentialité équivalentes, conformément à sa législation nationale. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après que ces organismes ont cessé leur activité.

Article 12
Tenue de journaux au niveau national

1. Les États membres veillent à ce que tout accès à des données à caractère personnel et tout échange de ces données avec le CS-SIS soient enregistrés dans le N.SIS afin de pouvoir contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS ainsi que l'intégrité et la sécurité des données. **Cela ne s'applique pas aux processus automatiques visés à l'article 4, paragraphe 4, points a), b) et c).**
2. Les journaux [...] indiquent, en particulier, l'historique du signalement, la date et l'heure de l'opération de traitement des données, les données utilisées pour effectuer une consultation, la référence des données transmises et les [...] **identificateurs d'utilisateur individuels et uniques**⁵⁵ de l'autorité compétente et de la personne chargée du traitement des données.
3. Si la consultation est effectuée à partir de données dactylo[...] **scopiques** ou d'une image faciale conformément à l'article [...] 42, les journaux indiquent, notamment, le type de données utilisées pour la consultation, le type de données transmises et les **identificateurs d'utilisateur individuels et uniques**⁵⁶ de l'autorité compétente et de la personne chargée du traitement des données.

⁵⁵ Libellé identique à celui du paragraphe 3 et de l'article 10, paragraphe 1, point f).

⁵⁶ Libellé identique à celui du paragraphe 2 et de l'article 10, paragraphe 1, point f).

4. Les journaux ne peuvent être utilisés que pour la finalité visée au paragraphe 1 et sont supprimés au plus tôt un an et au plus tard trois ans après leur création.
5. Les journaux peuvent être conservés plus longtemps s'ils sont nécessaires à une procédure de contrôle déjà engagée.
6. Les autorités **de contrôle** nationales [...] chargées de contrôler la licéité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du N.SIS ainsi que l'intégrité et la sécurité des données ont accès, dans les limites de leurs compétences et sur demande, à ces journaux afin de pouvoir s'acquitter de leurs tâches.
7. Lorsque les États membres procèdent à des recherches automatisées par scan de plaques minéralogiques via les systèmes de reconnaissance automatique des plaques minéralogiques, ils tiennent un journal de la recherche, en conformité avec leur législation nationale. [...] ⁵⁷ [...]

8.⁵⁸ La Commission adopte des actes d'exécution pour établir le contenu du journal visé au paragraphe 7. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

⁵⁷ Texte déplacé vers un nouveau paragraphe 8.

⁵⁸ Texte déplacé depuis le paragraphe 7.

Article 13

Autocontrôle

Les États membres veillent à ce que chaque autorité autorisée à avoir accès aux données du SIS prenne les mesures nécessaires pour se conformer au présent règlement et coopère, si nécessaire, avec l'autorité de contrôle nationale.

Article 14

Formation du personnel

Avant d'être autorisé à traiter des données stockées dans le SIS, puis à intervalles réguliers après avoir obtenu l'accès à ces données, le personnel des autorités qui a un droit d'accès au SIS reçoit une formation appropriée sur les règles en matière de sécurité et de protection des données et sur les procédures relatives au traitement des données fixées dans le manuel SIRENE. Ce personnel est informé des infractions et sanctions pénales éventuelles en la matière.

CHAPITRE III RESPONSABILITÉS DE L'AGENCE EU-LISA

Article 15

Gestion opérationnelle

1. L'agence eu-LISA est chargée de la gestion opérationnelle du SIS central. Elle veille, en coopération avec les États membres, à ce que le SIS central bénéficie en permanence de la [...] technologie **la plus appropriée**, sur la base d'une analyse coût-avantages.
2. Il incombe également à l'agence eu-LISA d'assurer les tâches ci-après en ce qui concerne l'infrastructure de communication:
 - a) supervision;
 - b) sécurité;
 - c) coordination des relations entre les États membres et le fournisseur.

3. La Commission est chargée de toutes les autres tâches liées à l'infrastructure de communication, en particulier:
 - a) les tâches relatives à l'exécution du budget;
 - b) les acquisitions et renouvellements;
 - c) les questions contractuelles.

4. L'agence eu-LISA est **également** chargée des tâches ci-après en ce qui concerne les bureaux SIRENE et la communication entre ces bureaux:
 - a) la coordination, [...] la gestion **et le soutien des activités de** test;
 - b) la gestion et la mise à jour des spécifications techniques relatives à l'échange d'informations supplémentaires entre les bureaux SIRENE et l'infrastructure de communication, ainsi que la gestion des effets des modifications techniques lorsqu'elles ont une incidence sur le SIS et sur les échanges d'informations supplémentaires entre les bureaux SIRENE.

5. L'agence eu-LISA élabore et gère un dispositif et des procédures de contrôle de qualité des données du CS-SIS et présente des rapports réguliers aux États membres. Elle présente à la Commission un rapport régulier indiquant les problèmes rencontrés et les États membres concernés. [...] ⁵⁹

⁵⁹ Texte déplacé vers un nouveau paragraphe 7.

6. La gestion opérationnelle du SIS central comprend toutes les tâches nécessaires pour que le SIS central puisse fonctionner 24 heures sur 24, 7 jours sur 7 **conformément au présent règlement**, en particulier les travaux de maintenance et les développements techniques indispensables au bon fonctionnement du système. Ces tâches incluent également **la coordination, la gestion et le soutien des** activités de test **concernant le SIS central et les systèmes nationaux**, destinées à vérifier que le SIS central et les systèmes nationaux fonctionnent conformément aux exigences techniques et fonctionnelles prévues à l'article 9 du présent règlement.

7.⁶⁰ La Commission adopte des actes d'exécution pour définir les exigences techniques relatives à l'infrastructure de communication visée au paragraphe 2, établir le dispositif et les procédures de contrôle de qualité des données du CS-SIS visés au paragraphe 5 et fixer l'interprétation relative à la qualité conforme des données. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 16

Sécurité - Agence eu-Lisa

1. L'agence eu-LISA adopte, pour le SIS central et l'infrastructure de communication, les mesures, dont un plan de sécurité, un plan de continuité des opérations et un plan de rétablissement après sinistre, propres à:
 - a) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;
 - b) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès aux installations);

⁶⁰ Texte déplacé depuis le paragraphe 5.

- c) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données);
- d) empêcher l'introduction non autorisée de données ainsi que tout examen, toute modification ou tout effacement non autorisés de données à caractère personnel stockées (contrôle du stockage);
- e) empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées au moyen de matériel de transmission de données (contrôle des utilisateurs);
- f) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des [...] **identificateurs** d'utilisateur individuels et uniques ainsi qu'à des modes d'accès confidentiels (contrôle de l'accès aux données);
- g) assurer la création de profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées en matière d'accès aux données ou aux installations de traitement de données, et la mise de ces profils à la disposition du Contrôleur européen de la protection des données visé à l'article 64, sans tarder et à la demande de celui-ci (profils des membres du personnel);
- h) garantir qu'il puisse être vérifié et constaté à quels organismes des données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données (contrôle de la transmission);
- i) garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, à quel moment et par qui (contrôle de l'introduction);
- j) empêcher, en particulier par des techniques de cryptage adaptées, que, lors de la transmission de données à caractère personnel ou du transport de support de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée (contrôle du transport);
- k) contrôler l'efficacité des mesures de sécurité visées au présent paragraphe et prendre les mesures d'organisation en matière de contrôle interne qui sont nécessaires au respect du présent règlement (autosurveillance).

2. L'agence eu-LISA prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la sécurité du traitement et de l'échange d'informations supplémentaires par l'intermédiaire de l'infrastructure de communication.

Article 17

Confidentialité - [...]Agence eu-Lisa

1. Sans préjudice de l'article 17 du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne, l'agence eu-LISA applique des règles appropriées en matière de secret professionnel, ou impose des obligations de confidentialité équivalentes, qui s'appliquent à tous les membres de son personnel appelés à travailler avec des données du SIS et répondent à des normes comparables à celles prévues à l'article 11 du présent règlement. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la fin de leurs activités.
2. L'agence eu-LISA prend des mesures équivalentes à celles visées au paragraphe 1 pour assurer la confidentialité de l'échange d'informations supplémentaires par l'intermédiaire de l'infrastructure de communication.

Article 18

Tenue de journaux au niveau central

1. L'agence eu-LISA veille à ce que tous les accès aux données à caractère personnel et tous les échanges de telles données contenues dans le CS-SIS soient enregistrés aux fins mentionnées à l'article 12, paragraphe 1.
2. Les journaux indiquent, en particulier, l'historique [...] du **signalement**⁶¹, la date et l'heure de la transmission des données, les [...] données utilisées pour effectuer des consultations, la référence des données transmises et les [...] **identificateurs d'utilisateur individuels et uniques**⁶² de l'autorité compétente chargée du traitement des données.

⁶¹ Au singulier, comme à l'article 12, paragraphe 2.

⁶² Libellé identique à celui de l'article 10, paragraphe 1, point f), et de l'article 12, paragraphes 2 et 3.

3. Si la consultation est effectuée à partir de données dactylo[...] **scopiques** ou d'une image faciale conformément aux articles 40, 41 et 42, les journaux indiquent, notamment, le type de données utilisées pour la consultation, une référence au type de données transmises et les [...] **identificateurs d'utilisateur individuels et uniques** de l'autorité compétente et de la personne chargée du traitement des données.
4. Les journaux ne peuvent être utilisés qu'aux fins mentionnées au paragraphe 1, et sont supprimés au plus tôt un an et au plus tard trois ans après leur création. Les journaux contenant l'historique des signalements sont effacés de un à trois ans après la suppression des signalements.
5. Les journaux peuvent être conservés plus longtemps s'ils sont nécessaires à une procédure de contrôle déjà engagée.
6. Le [...] **Contrôleur européen de la protection des données** a accès, dans les limites de [...] **ses** compétences et à [...] **sa** demande, à ces journaux afin de pouvoir s'acquitter de [...] **ses** tâches.

CHAPITRE IV

INFORMATION DU PUBLIC

Article 19

Campagne d'information sur le SIS

La Commission, en coopération avec les autorités de contrôle nationales et le Contrôleur européen de la protection des données, organise régulièrement des campagnes visant à faire connaître au public les objectifs du SIS, les données stockées, les autorités disposant d'un droit d'accès au SIS et les droits des personnes concernées. Les États membres, en coopération avec leurs autorités de contrôle nationales, élaborent et mettent en œuvre les politiques nécessaires pour assurer l'information générale de leurs citoyens sur le SIS.

CHAPITRE V

CATÉGORIES DE DONNÉES ET APPOSITION D'UN INDICATEUR DE VALIDITÉ

Article 20

Catégories de données

1. Sans préjudice des dispositions de l'article 8, paragraphe 1, ou des dispositions du présent règlement prévoyant le stockage de données complémentaires, le SIS comporte exclusivement les catégories de données qui sont fournies par chacun des États membres et qui sont nécessaires aux fins prévues aux articles 26, 32, 34, 36, [...] 38 **et 40**.
2. Les catégories de données sont les suivantes:
 - a) les renseignements sur les personnes signalées;
 - b) les renseignements sur les objets visés aux articles **26**, 32, **34**, 36 et 38.
3. **Tout signalement dans le SIS qui comporte** [...] des renseignements concernant des personnes [...] comprend uniquement les données suivantes
 - a) le[...]s nom[...]s;
 - b) le[...]s prénom[...]s;
 - c) le[...]s nom[...]s à la naissance;
 - d) les noms utilisés antérieurement et les pseudonymes;
 - e) les signes physiques particuliers, objectifs et inaltérables;
 - f) le lieu de naissance;

- g) la date de naissance;
- h) le [...] **genre**;
- i) la ou les nationalités;
- j) l'indication que la personne concernée:
 - i. est armée; [...]
 - ii. **est** violente [...];
 - iii. **s'est enfuie ou échappée;**
 - iv. **présente un risque de suicide;**
 - v. **représente une [...] **menace pour la santé publique; ou****
 - vi. est impliquée dans une activité [...] **liée au terrorisme;**
- k) le motif du signalement;
- l) l'autorité signalante;
- m) une référence à la décision qui est à l'origine du signalement;
- n) la conduite à tenir;
- o) le(s) lien(s) vers d'autres signalements introduits dans le SIS conformément à l'article [...] **60**;
- p) le type d'infraction pour lequel le signalement a été introduit;
- q) le numéro d'immatriculation de la personne dans un registre national;

- r) la catégorie de personne disparue (seulement pour les signalements visés à l'article 32);
 - s) la catégorie **des** documents d'identification de la personne;
 - t) le pays de délivrance **des** documents d'identification de la personne;
 - u) le(s) numéro(s) **des** documents d'identification de la personne;
 - v) la date de délivrance **des** documents d'identification de la personne;
 - w) les photographies et les images faciales;
 - x) les profils ADN, dans les cas prévus à l'article 22, paragraphe 1, point b), du présent règlement;
 - y) les données dactylo[...]**scopiques**;
 - z) une copie, **si possible en couleurs, des** documents d'identification.
4. Les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées aux paragraphes 2 et 3 sont établies et précisées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 72, paragraphe 2.
5. [...] ⁶³ Ces règles techniques sont similaires pour les consultations dans le CS-SIS, dans les copies nationales **ou partagées** et dans les copies techniques visées à l'article 53, paragraphe 2, et elles sont fondées sur des normes communes établies et précisées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 72, paragraphe 2.

⁶³ Fait double emploi avec le paragraphe 4.

Article 21
Proportionnalité

1. Avant d'introduire un signalement et de prolonger la durée de validité de ce dernier, les États membres vérifient si le dossier est suffisamment approprié, pertinent et important pour justifier [...] **l'existence** d'un signalement dans le SIS.

2. Si un État membre recherche une personne ou un objet en rapport avec une infraction qui relève des articles [...] **3 à 14** de la **directive 2017/541 ou qui est équivalente à l'une de ces infractions** [...] ⁶⁴, il crée [...] le signalement correspondant [...]. **À titre exceptionnel, les États membres peuvent s'abstenir de créer le signalement si celui-ci risque de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires liées à la sécurité publique ou nationale.**

Article 22⁶⁵

[...]

⁶⁴ [...]

⁶⁵ Article déplacé vers un nouveau chapitre XI *bis*, en tant qu'article 41 *bis*.

[...]

Article 23

Exigence à remplir pour l'introduction d'un signalement

1. [...] ⁶⁶ **Toutes les données énumérées à l'article 20, paragraphe 3, sont introduites, lorsqu'elles sont disponibles**⁶⁷.
2. [...] ⁶⁸ Un signalement concernant une personne ne peut être introduit sans les données mentionnées à l'article 20, paragraphe 3, points a), g), k), et [...] n), [...], sauf dans les situations visées à l'article 40⁶⁹.

⁶⁶ Déplacé en partie vers le paragraphe 2.

⁶⁷ Déplacé en partie depuis le paragraphe 2.

⁶⁸ Déplacé en partie vers le paragraphe 1.

⁶⁹ Déplacé en partie depuis le paragraphe 1.

Article 24

Dispositions générales concernant l'apposition d'un indicateur de validité

1. Si un État membre estime que la mise en œuvre d'un signalement introduit conformément aux articles 26, 32 **ou** [...] 36 n'est pas compatible avec son droit national, ses obligations internationales ou des intérêts nationaux essentiels, il peut exiger par la suite que soit apposé sur ledit signalement un indicateur de validité visant à ce que l'exécution de la conduite à tenir demandée dans le signalement n'ait pas lieu sur son territoire. L'indicateur de validité est apposé par le bureau SIRENE de l'État membre signalant.
2. Afin de permettre à un État membre de demander qu'un indicateur de validité soit apposé sur un signalement introduit conformément à l'article 26, tous les États membres sont informés automatiquement, par voie d'échange d'informations supplémentaires, de tout nouveau signalement relevant de cette catégorie.
3. Si, dans des cas particulièrement urgents et graves, un État membre signalant demande l'exécution de la conduite à tenir, l'État membre d'exécution examine s'il peut autoriser le retrait de l'indicateur de validité qui a été apposé à sa demande. Si l'État membre d'exécution est en mesure de le faire, il prend les dispositions nécessaires afin que la conduite à tenir puisse être exécutée sans délai.

Article 25

Apposition d'un indicateur de validité sur les signalements en vue d'une arrestation aux fins de remise

1. Lorsque la décision-cadre 2002/584/JAI s'applique, l'indicateur de validité visant à prévenir une arrestation est [...] apposé sur un signalement en vue d'une arrestation aux fins de remise si l'autorité judiciaire compétente en vertu de la législation nationale pour l'exécution d'un mandat d'arrêt européen a refusé cette exécution en invoquant un motif de non-exécution et si l'apposition de l'indicateur de validité a été demandée.

Un État membre peut également demander qu'un indicateur de validité soit apposé sur le signalement si son autorité judiciaire compétente remet en liberté la personne visée par le signalement au cours de la procédure de remise.

2. Toutefois, à la demande d'une autorité judiciaire compétente en vertu de la législation nationale, l'apposition d'un indicateur de validité sur un signalement en vue d'une arrestation aux fins de remise peut également être demandée si, sur la base d'une instruction générale ou dans un cas particulier, il est évident que l'exécution du mandat d'arrêt européen devra être refusée.

CHAPITRE VI

SIGNALEMENTS DES PERSONNES RECHERCHÉES EN VUE D'UNE ARRESTATION AUX FINS DE REMISE OU D'EXTRADITION

Article 26

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données relatives aux personnes recherchées en vue d'une arrestation aux fins de remise sur la base d'un mandat d'arrêt européen ou en vue d'une arrestation aux fins d'extradition sont introduites à la demande de l'autorité judiciaire de l'État membre signalant.
2. Les données relatives aux personnes recherchées en vue d'une arrestation aux fins de remise sont également introduites sur la base des mandats d'arrêt émis conformément aux accords conclus entre l'Union et des pays tiers sur le fondement de l'article 37 du traité sur l'Union européenne, aux fins de la remise de personnes sur la base d'un mandat d'arrêt, qui prévoient la transmission d'un tel mandat d'arrêt par l'intermédiaire du SIS.
3. Toute référence, dans le présent règlement, à des dispositions de la décision-cadre 2002/584/JAI est réputée inclure les dispositions correspondantes des accords conclus entre l'Union européenne et des pays tiers sur le fondement de l'article 37 du traité sur l'Union européenne, aux fins de la remise de personnes sur la base d'un mandat d'arrêt, qui prévoient la transmission d'un tel mandat d'arrêt par l'intermédiaire du SIS.

4. [...] **En cas d'opérations de recherche en cours [...], l'État membre signalant peut rendre temporairement non consultable un signalement en vue d'une arrestation introduit en vertu de l'article 26, de sorte que l'utilisateur final dans les États membres concernés par l'opération ne puisse consulter ce signalement et que ce dernier ne soit accessible qu'aux bureaux SIRENE, lorsque les conditions ci-après sont remplies:**

- a) [...] **le but de l'opération ne peut pas être atteint par d'autres mesures;**
- b) [...] **une autorisation préalable a été donnée par** l'autorité judiciaire compétente de l'État membre signalant; **et**
- c) **tous les États membres concernés par l'opération ont été informés par voie d'échange d'informations supplémentaires.**

[...] **La** fonctionnalité **prévue au premier alinéa n'**est utilisée **que** pour une période n'excédant pas 48 heures [...]. **Toutefois, si** cela est nécessaire sur le plan opérationnel, son utilisation peut [...] être prolongée pour d'autres périodes de 48 heures. Les États membres tiennent des statistiques concernant le nombre de signalements pour lesquels cette fonctionnalité a été employée.

5. Lorsqu'il existe des indices manifestes de l'existence d'un lien entre un objet visé à l'article 38, paragraphe 2, points a), b), c), e), g), h) et k), et une personne faisant l'objet d'un signalement en vertu des paragraphes 1 et 2, un signalement relatif à cet objet peut être introduit pour retrouver la personne. Dans ce cas, le signalement de la personne et le signalement de l'objet sont mis en relation conformément à l'article 60.

6. La Commission adopte des actes d'exécution pour établir et préciser les règles nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 5. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 27

Données complémentaires concernant les personnes recherchées en vue d'une arrestation aux fins de remise

1. Si une personne est recherchée en vue d'une arrestation aux fins de remise sur la base d'un mandat d'arrêt européen, l'État membre signalant introduit dans le SIS une copie de l'original du mandat d'arrêt européen.
2. L'État membre signalant peut ajouter une copie de la traduction du mandat d'arrêt européen dans une ou plusieurs autres langues officielles des institutions de l'Union européenne.

Article 28

Informations supplémentaires concernant les personnes recherchées en vue d'une arrestation aux fins de remise

L'État membre qui a introduit le signalement dans le SIS en vue d'une arrestation aux fins de remise communique aux autres États membres les informations mentionnées à l'article 8, paragraphe 1, de la décision-cadre 2002/584/JAI par voie d'échange d'informations supplémentaires.

Article 29

Informations supplémentaires concernant les personnes recherchées en vue d'une arrestation aux fins d'extradition

1. L'État membre qui a introduit le signalement dans le SIS en vue d'une extradition communique aux autres États membres les données ci-après par voie d'échange d'informations supplémentaires:
 - a) l'autorité dont émane la demande d'arrestation;

- b) l'existence d'un mandat d'arrêt ou d'un acte ayant la même force, ou d'un jugement exécutoire;
 - c) la nature et la qualification légale de l'infraction;
 - d) la description des circonstances de la commission de l'infraction, y compris le moment, le lieu et le degré de participation à l'infraction de la personne signalée;
 - e) dans la mesure du possible, les conséquences de l'infraction;
 - f) toute autre information utile ou nécessaire à l'exécution de la conduite à tenir demandée dans le signalement.
2. Les données citées au paragraphe 1 ne sont pas communiquées lorsque les données visées aux articles 27 ou 28 ont déjà été fournies et sont considérées comme suffisantes pour l'exécution de la conduite à tenir demandée dans le signalement par l'État membre concerné.

Article 30

Conversion des signalements concernant des personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition

S'il n'est pas possible de procéder à une arrestation soit en raison du refus opposé par un État membre requis conformément aux procédures relatives à l'apposition d'un indicateur de validité prévues aux articles 24 et 25, soit parce que, dans le cas d'un signalement en vue d'une arrestation aux fins d'extradition, une enquête n'est pas encore terminée, l'État membre requis traite le signalement comme [...] un signalement aux fins de communication du lieu où se trouve la personne concernée.

Article 31

Exécution de la conduite à tenir demandée dans le signalement d'une personne recherchée en vue d'une arrestation aux fins de remise ou d'extradition

1. Un signalement introduit dans le SIS conformément à l'article 26, associé aux données complémentaires visées à l'article 27, constitue un mandat d'arrêt européen émis conformément à la décision-cadre 2002/584/JAI et produit les mêmes effets qu'un tel mandat, lorsque ladite décision s'applique.
2. Lorsque la décision-cadre 2002/584/JAI ne s'applique pas, un signalement introduit dans le SIS conformément aux articles 26 et 29 a la même force qu'une demande d'arrestation provisoire au sens de l'article 16 de la convention européenne d'extradition du 13 décembre 1957 ou de l'article 15 du traité Benelux d'extradition et d'entraide judiciaire en matière pénale du 27 juin 1962.

CHAPITRE VII

SIGNALEMENTS DES PERSONNES DISPARUES OU VULNÉRABLES

Article 32

Objectifs des signalements et conditions auxquelles ils sont soumis

1. [...]

2. Les catégories ci-après de personnes [...] **sont** [...] introduites **dans le SIS à la demande d'une autorité compétente de l'État membre signalant:**
- a) les personnes disparues devant être placées sous protection
 - i) dans l'intérêt de leur propre protection;
 - ii) pour la prévention de menaces;
 - b) les personnes disparues ne devant pas être placées sous protection;
 - c) les enfants risquant d'être enlevés conformément au paragraphe 4 **qui doivent être empêchés de voyager; ou**
 - d) les personnes vulnérables qui doivent être empêchées de voyager pour leur propre protection conformément au paragraphe 4 bis.**
3. **Les points a) et d) du** [...] paragraphe 2 [...] s'appliquent en particulier aux enfants, **ainsi qu'aux** personnes **au sujet desquelles une** décision **a été prise par les** [...] autorités compétentes.

4. Un signalement concernant un enfant visé au paragraphe 2, point c), est introduit, à la demande des [...] autorités [...] compétentes, **y compris des autorités judiciaires des États membres ayant compétence en matière de responsabilité parentale, [...]**⁷⁰ lorsqu'il existe un risque concret et manifeste que l'enfant soit déplacé, de manière illégale [...], hors de l'État membre où se trouvent **nt** [...] **ces** autorités [...] compétentes. [...]

L'autorité compétente examine régulièrement la nécessité de maintenir le signalement.

4 bis. Un signalement concernant les personnes vulnérables visées au paragraphe 2, point d), est introduit, à la demande des autorités compétentes, lorsqu'il est considéré que ces personnes courraient un risque concret et manifeste si elles quittaient l'État membre concerné. [...]

L'autorité compétente examine régulièrement la nécessité de maintenir le signalement.

⁷⁰ [...]

5. Les États membres veillent à ce que les données introduites dans le SIS précisent à quelle catégorie mentionnée au paragraphe 2 appartient la personne [...]. En outre, les États membres veillent à ce que les données introduites dans le SIS indiquent quel est le type de dossier [...] concerné **et, en ce qui concerne les signalements introduits en vertu du paragraphe 2, points c) et d), à ce que toutes les informations pertinentes soient mises à disposition au sein du bureau SIRENE de l'État membre signalant lors de la création du signalement.** [...] ⁷¹
6. Quatre mois avant qu'un enfant faisant l'objet d'un signalement en vertu du présent article n'atteigne **l'âge de la majorité conformément au droit national de l'État membre signalant** [...], le CS-SIS avertit automatiquement l'État membre signalant que le motif de la demande et la conduite à tenir doivent être actualisés ou que le signalement doit être supprimé.
7. Lorsqu'il existe des indices manifestes de l'existence d'un lien entre des véhicules, bateaux ou aéronefs et une personne faisant l'objet d'un signalement en vertu du paragraphe 2, des signalements relatifs à ces véhicules, bateaux ou aéronefs peuvent être introduits pour retrouver la personne. Dans ce cas, le signalement de la personne [...] et le signalement de l'objet sont mis en relation conformément à l'article 60. [...] ⁷²

⁷¹ Déplacé vers le paragraphe 8.

⁷² Déplacé vers le paragraphe 8.

8.⁷³ La Commission adopte des actes d'exécution pour établir et préciser les règles de catégorisation des types de dossier et de saisie des données visées au paragraphe 5 ainsi que les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 7. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 33

Exécution de la conduite à tenir demandée dans un signalement

1. Lorsqu'une personne visée à l'article 32 est retrouvée, les autorités compétentes communiquent le lieu où elle se trouve à l'État membre signalant, sous réserve des dispositions du paragraphe 2.

1 bis. Dans le cas [...] **des personnes** qui doivent être placées sous protection **conformément à l'article 32, paragraphe 2, points a), c) et d)**, l'État membre d'exécution consulte immédiatement **ses propres autorités compétentes ainsi que celles de** l'État membre signalant **par voie d'échange d'informations supplémentaires** afin de décider sans délai des mesures à prendre pour préserver l'intérêt supérieur de l'enfant. Les autorités compétentes **de l'État membre d'exécution** peuvent, **conformément au droit national** [...], placer les personnes concernées en sécurité aux fins de les empêcher de poursuivre leur voyage [...].

2. La communication de données, autre que celle qui a lieu entre les autorités compétentes, concernant une personne majeure disparue qui a été retrouvée est subordonnée au consentement de cette personne. Les autorités compétentes peuvent cependant indiquer à la personne qui a signalé la disparition que le signalement a été effacé, du fait que la personne disparue a été localisée.

⁷³ Déplacé depuis le paragraphe 5 in fine et le paragraphe 7 in fine.

CHAPITRE VIII
SIGNALEMENTS DES PERSONNES RECHERCHÉES DANS LE BUT DE RENDRE
POSSIBLE LEUR CONCOURS DANS LE CADRE D'UNE PROCÉDURE JUDICIAIRE

Article 34

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Aux fins de la communication du lieu de séjour ou du domicile de personnes, les États membres introduisent dans le SIS, à la demande d'une autorité compétente, des données relatives:
 - a) aux témoins;
 - b) aux personnes citées à comparaître ou recherchées pour être citées à comparaître devant les autorités judiciaires dans le cadre d'une procédure pénale afin de répondre de faits pour lesquels elles font l'objet de poursuites;
 - c) aux personnes qui doivent faire l'objet d'une notification d'un jugement en matière pénale ou d'autres documents en rapport avec une procédure pénale afin de répondre de faits pour lesquels elles font l'objet de poursuites;
 - d) aux personnes qui doivent faire l'objet d'une demande de se présenter pour subir une peine privative de liberté.

2. Lorsqu'il existe des indices manifestes de l'existence d'un lien entre des véhicules, bateaux ou aéronefs et une personne faisant l'objet d'un signalement en vertu du paragraphe 1, des signalements relatifs à ces véhicules, bateaux ou aéronefs peuvent être introduits pour localiser la personne. Dans ce cas, le signalement de la personne et le signalement de l'objet sont mis en relation conformément à l'article 60. [...] ⁷⁴.

⁷⁴ Déplacé vers le paragraphe 3.

3.⁷⁵ La Commission adopte des actes d'exécution pour établir et préciser les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 35

Exécution de la conduite à tenir demandée dans un signalement

Les renseignements demandés sont communiqués à l'État membre demandeur par voie d'échange d'informations supplémentaires.

CHAPITRE IX

SIGNALEMENTS DES PERSONNES OU DES OBJETS AUX FINS DE CONTRÔLE DISCRET, DE CONTRÔLE D'INVESTIGATION OU DE CONTRÔLE SPÉCIFIQUE

Article 36

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données concernant des personnes ou **les objets visés à l'article 38, paragraphe 2, points a), b), c), e), g), h), j) et k), ainsi que des moyens de paiement autres que les espèces** sont introduites conformément au droit national de l'État membre signalant, aux fins de contrôle discret, de contrôle d'investigation ou de contrôle spécifique, conformément à l'article 37, paragraphes **3**, 4 et **5**.

1 bis. Lors de l'introduction de signalements aux fins de contrôle discret, de contrôle d'investigation ou de contrôle spécifique et lorsque les informations demandées par l'État membre signalant viennent s'ajouter à celles prévues à l'article 37, paragraphe 1, l'État membre signalant ajoute au signalement toutes les informations demandées.

⁷⁵ Déplacé depuis le paragraphe 2 in fine.

2. Le signalement peut être introduit **à des fins de prévention, de détection, d'enquête et de poursuites concernant des infractions pénales, pour l'exécution d'une condamnation pénale et pour la prévention de menaces pour la sécurité publique:**
- a) lorsqu'il existe des indices manifestes laissant supposer qu'une personne a l'intention de commettre ou commet une infraction grave, en particulier une des infractions mentionnées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI; **ou**
 - b) lorsque les informations mentionnées à l'article 37, paragraphe 1, sont nécessaires pour l'exécution de la **sanction** [...] pénale prononcée à l'encontre d'une personne reconnue coupable d'une infraction grave, en particulier une des infractions mentionnées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI; ou
 - c) lorsque l'appréciation globale portée sur une personne, en particulier sur la base des infractions pénales commises jusqu'alors, laisse supposer qu'elle pourrait également commettre à l'avenir des infractions graves, en particulier une des infractions mentionnées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI.
3. En outre, le signalement peut être effectué conformément au droit national, à la demande des instances compétentes pour la sûreté de l'État, lorsque des indices concrets laissent supposer que les informations visées à l'article 37, paragraphe 1, sont nécessaires à la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'État. L'État membre introduisant le signalement en vertu du présent paragraphe en tient informés les autres États membres. Chaque État membre détermine à quelles autorités cette information est transmise **par l'intermédiaire de son bureau SIRENE.**
4. Lorsqu'il existe des indices manifestes de l'existence d'un lien entre **des objets visés à l'article 38, paragraphe 2, points a), b), c), e), g), h), j) et k), ou des moyens de paiement autres que les espèces** [...] et des infractions graves visées au paragraphe 2 ou des menaces graves visées au paragraphe 3, des signalements relatifs à ces **objets** [...] peuvent être introduits **et mis en relation avec les signalements introduits en vertu des paragraphes 2 et 3.**

5. [...] ⁷⁶ [...]

6.⁷⁷ La Commission adopte des actes d'exécution pour établir et préciser les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 4 ainsi que des informations complémentaires visées au paragraphe 1 bis. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 37

Exécution de la conduite à tenir demandée dans un signalement

1. Dans le cadre des contrôles discrets, des contrôles d'investigation ou des contrôles spécifiques, les informations ci-après sont, en tout ou en partie, recueillies et transmises à [...] l'État membre signalant [...]:
 - a) le fait que la personne signalée, **les objets signalés visés à l'article 38, paragraphe 2, points a), b), c), e), g), h), j) et k), ou les moyens de paiement signalés autres que les espèces a ou ont** été retrouvés(s);
 - b) le lieu, l'heure et la raison du contrôle;

⁷⁶ Déplacé vers le paragraphe 6.

⁷⁷ Déplacé depuis le paragraphe 5 in fine.

- c) l'itinéraire suivi et la destination visée;
- d) les personnes qui accompagnent l'intéressé ou les occupants du véhicule, du bateau ou de l'aéronef ou les personnes qui accompagnent le détenteur du document officiel vierge ou du document d'identité délivré, dont il est permis de supposer qu'ils sont associés à l'intéressé;
- e) l'identité révélée et la description de la personne ayant fait usage du document officiel vierge ou du document d'identité délivré faisant l'objet du signalement;
- f) **les objets visés à l'article 38, paragraphe 2, points a), b), c), e), g), h), j) et k), ou les moyens de paiement autres que les espèces** [...] utilisés;
- g) les objets transportés, y compris les documents de voyage;
- h) les circonstances dans lesquelles la personne, le véhicule **à moteur, la remorque, la caravane**, le bateau, **le conteneur**, l'aéronef, le document officiel vierge, les documents d'identité délivrés **ou les moyens de paiements autres que les espèces** a **ou ont** été retrouvés**(s)**;
- i) **les autres informations dont le recueil a été demandé par l'État membre signalant conformément à l'article 36, paragraphe 1 bis.**

2. Les informations visées au paragraphe 1 sont communiquées par voie d'échange d'informations supplémentaires.
3. [...] **Un contrôle discret comprend le recueil discret d'autant d'informations décrites au paragraphe 1 que possible au cours des activités de routine menées par les autorités nationales compétentes. Le recueil de ces informations ne met pas en péril le caractère discret des contrôles et la personne visée par le signalement n'est en aucune manière informée de l'existence du signalement.**

4. [...] Un contrôle d'investigation comprend [...] l'audition de la personne [...]⁷⁸, **notamment sur la base des informations ou des questions spécifiques ajoutées au signalement par l'État membre signalant. L'audition est menée conformément au droit national de l'État membre d'exécution.** [...]
5. Pendant les contrôles spécifiques, les personnes, les véhicules, les bateaux, les aéronefs, les conteneurs et les objets transportés peuvent être fouillés [...] aux fins visées à l'article 36. Les fouilles sont exécutées conformément au droit national. [...]⁷⁹
- 6.** Si le contrôle spécifique n'est pas autorisé par la législation [...] **nationale**, il est remplacé par un contrôle d'investigation dans l'État membre concerné⁸⁰. **Si le contrôle d'investigation n'est pas autorisé par la législation nationale, il est remplacé par un contrôle discret dans l'État membre concerné**⁸¹.
- 7.** **Le paragraphe 6 s'applique sans préjudice de l'obligation incombant aux États membres de mettre à la disposition des utilisateurs finaux toutes les informations complémentaires visées à l'article 36, paragraphe 1 bis, et de veiller à ce que ces informations soient recueillies et communiquées à l'État membre signalant par voie d'échange d'informations supplémentaires.**

⁷⁸ Déplacé vers un nouveau paragraphe 6.

⁷⁹ Déplacé vers un nouveau paragraphe 6.

⁸⁰ Déplacé depuis le paragraphe 5.

⁸¹ Déplacé depuis le paragraphe 4.

CHAPITRE X

SIGNALEMENTS DES OBJETS AUX FINS D'UNE SAISIE OU DE LA PREUVE DANS UNE PROCÉDURE PÉNALE

Article 38

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données relatives aux objets recherchés aux fins d'une saisie [...] ou de la preuve dans une procédure pénale sont introduites dans le SIS.
2. Les catégories ci-après d'objets facilement identifiables sont introduites:
 - a) les véhicules à moteur [...], indépendamment de leur système de propulsion;
 - b) les remorques d'un poids à vide supérieur à 750 kg;
 - c) les caravanes;
 - d) le matériel industriel;
 - e) les bateaux;
 - f) les moteurs de bateaux;
 - g) les conteneurs;
 - h) les aéronefs;
 - h bis) les moteurs d'aéronefs;**
 - i) les armes à feu;

- j) les documents officiels vierges volés, détournés, [...] égarés **ou qui sont des faux**;
- k) les documents d'identité délivrés tels que les passeports, cartes d'identité, [...] titres de séjour, [...] documents de voyage **et permis de conduire** qui ont été volés, détournés, égarés, invalidés ou qui sont [...] **des faux**;
- l) les certificats d'immatriculation et les plaques d'immatriculation qui ont été volés, détournés, égarés, invalidés ou qui sont [...] **des faux**;
- m) les billets de banque (billets enregistrés) et les **faux** billets de banque [...];
- n) [...] les produits informatiques [...] ⁸²;
- o) les composants identifiables de véhicules à moteur;
- p) les composants identifiables de matériel industriel;
- q) **les autres objets identifiables de grande valeur⁸³, tels qu'ils sont définis conformément au paragraphe 3.**

En ce qui concerne les documents visés au paragraphe 2, points j), k) et l), l'État membre signalant peut préciser si ces documents ont été volés, détournés, égarés, invalidés ou s'ils sont des faux.

⁸² Déplacé vers un nouveau point q).

⁸³ Déplacé depuis le point n).

3. La définition des nouvelles sous-catégories d'objets figurant au paragraphe 2, points n), o), p) et q), et les règles techniques nécessaires pour l'introduction, la mise à jour, la suppression et la consultation des données visées au paragraphe 2 sont établies et précisées au moyen de mesures d'exécution conformément à la procédure d'examen visée à l'article 72, paragraphe 2.

Article 39

Exécution de la conduite à tenir demandée dans un signalement

1. Lorsqu'une consultation fait apparaître l'existence d'un signalement correspondant à un objet retrouvé, l'autorité qui a établi la concordance entre les deux données procède à la saisie de l'objet conformément au droit national et se met en rapport avec l'autorité signalante afin de convenir des mesures à prendre. À cette fin, des données à caractère personnel peuvent également être transmises conformément au présent règlement.
2. Les informations mentionnées au paragraphe 1 sont communiquées par voie d'échange d'informations supplémentaires.
3. L'État membre qui a retrouvé l'objet prend les mesures demandées conformément à son droit national.

CHAPITRE XI

SIGNALEMENTS DES PERSONNES RECHERCHÉES INCONNUES À DES FINS D'IDENTIFICATION CONFORMÉMENT AU DROIT NATIONAL [...] ⁸⁴

Article 40

*Signalements des personnes recherchées inconnues à des fins [...] **d'identification** conformément au droit national*

Des données dactylo[...] **scopiques** qui ne sont pas liées à des personnes faisant l'objet de signalements peuvent être saisies dans le SIS. Ces données dactylo[...] **scopiques** consistent en des séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires **qui sont** découvertes sur les lieux d'infractions **graves ou d'infractions terroristes** faisant l'objet d'une enquête, [...] lorsqu'il peut être établi, avec un degré élevé de probabilité, qu'elles appartiennent à [...] **un** auteur de l'infraction.

Les données dactylo[...] **scopiques** relevant de cette catégorie sont stockées avec la mention "personne ou suspect recherché inconnu" **et ne sont stockées que si** [...] les autorités compétentes **de l'État membre signalant** ne peuvent pas établir l'identité de la personne en recourant à toute autre base de données nationale, européenne ou internationale.

Article 41

Exécution de la conduite à tenir demandée dans un signalement

En cas de réponse positive [...] après consultation des données stockées en vertu de l'article 40, l'identité de la personne est établie conformément au droit national, avec vérification **par un expert** que les données dactylo[...] **scopiques** stockées dans le SIS appartiennent à la personne. Les États membres communiquent **les informations sur l'identité de la personne et le lieu où elle se trouve** par voie d'échange d'informations supplémentaires pour faciliter l'instruction en temps voulu du dossier.

⁸⁴ Déplacé vers un nouveau chapitre XI bis.

CHAPITRE XI bis
RÈGLES PARTICULIÈRES POUR LES DONNÉES BIOMÉTRIQUES

*Article **41 bis (ex-article 22)***

Règles particulières pour l'introduction de photographies, d'images faciales, de données dactylo[...]scopiques et de profils ADN

1. L'introduction dans le SIS des données mentionnées à l'article 20, paragraphe 3, points w), x) et y), est soumise aux dispositions suivantes:
 - a) les photographies, les images faciales, les données dactylo[...]scopiques et les profils ADN ne sont introduits qu'après avoir été soumis à un contrôle de qualité visant à garantir le respect de normes minimales en matière de qualité des données;
 - b) un profil ADN ne peut être ajouté qu'aux signalements prévus à l'article 32, paragraphe 2, points a) et c), et seulement lorsque des photographies, images faciales ou données dactylo[...]scopiques permettant une identification ne sont pas disponibles **ou ne sont pas suffisantes**. Le profil ADN de personnes qui sont des ascendants ou descendants directs ou des frères ou sœurs de la personne signalée peut être ajouté au signalement à condition que ces personnes concernées donnent leur consentement explicite. [...]

2. Des normes de qualité sont définies pour le stockage des données visées au paragraphe 1, point a), du présent article et à l'article 40. Leur contenu est déterminé au moyen de mesures d'exécution et mis à jour conformément à la procédure d'examen visée à l'article 72, paragraphe 2.

Article 42

Règles spécifiques pour les vérifications ou les consultations à l'aide de photographies, d'images faciales, de données dactylo[...]scopiques et de profils ADN

1. Les photographies, les images faciales, les données dactylo[...]scopiques et les profils ADN sont extraits du SIS, **chaque fois que c'est nécessaire**, pour vérifier l'identité d'une personne localisée à la suite d'une consultation alphanumérique effectuée dans le SIS.
2. [...] **Si** l'identité de la personne ne peut être établie par d'autres moyens, **les données dactyloscopiques** [...] **sont consultées à des fins d'identification**. Les données dactylo[...]scopiques peuvent [...] **dans tous les cas être consultées** pour identifier une personne.
3. Les données dactylo[...]scopiques stockées dans le SIS en rapport avec des signalements introduits en vertu des articles 26, **32**, 34 [...], **36** et [...] **40** peuvent également faire l'objet de consultations à l'aide de séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires découvertes sur les lieux d'infractions **graves ou d'infractions terroristes**⁸⁵ faisant l'objet d'une enquête, lorsqu'il peut être établi, avec un degré élevé de probabilité, qu'elles appartiennent à [...] **un** auteur de l'infraction [...].
4. Dès que cela est techniquement possible tout en assurant un haut degré de fiabilité de l'identification, les photographies et les images faciales peuvent être utilisées pour identifier une personne. **Avant que cette fonctionnalité soit introduite, la Commission présente un rapport précisant si la technique requise est disponible et prête à être employée; le Parlement européen est consulté.**⁸⁶ L'identification à l'aide de photographies ou d'images faciales [...] est utilisée **sous réserve du droit national** [...].

⁸⁵ Libellé correspondant à celui de l'article 40.

⁸⁶ Libellé similaire à celui de l'article 22, point c), du règlement (CE) n° 1987/2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

CHAPITRE XII

DROIT D'ACCÈS ET CONSERVATION DES SIGNALEMENTS

Article 43

Autorités disposant d'un droit d'accès aux signalements

1. **Les autorités nationales compétentes ont** [...] accès aux données introduites dans le SIS ainsi que le droit de les consulter, directement ou dans une copie, [...] **aux fins**:
 - a) du contrôle aux frontières, conformément au règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen);
 - b) des vérifications de police et de douanes effectuées à l'intérieur de l'État membre concerné et de la coordination de celles-ci par les autorités désignées;
 - c) des autres actions [...] menées à des fins de prévention et de détection des infractions pénales, [...] d'enquêtes **ou de poursuites** en la matière **ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique ou nationale et la prévention de telles menaces dans** l'État membre concerné⁵⁹;
 - d) de l'examen des conditions et de l'adoption des décisions relatives à l'entrée et au séjour des ressortissants de pays tiers sur le territoire des États membres, [...] en ce qui concerne les titres de séjour et les visas de long séjour, ainsi qu'au retour des ressortissants de pays tiers;
 - e) **des vérifications portant sur les ressortissants de pays tiers qui entrent ou séjournent illégalement sur le territoire des États membres, ainsi que sur les demandeurs de protection internationale.**

1 bis. Le droit d'accès aux données introduites dans le SIS et le droit de les consulter directement peuvent être exercés par les autorités nationales compétentes en matière de naturalisation, dans l'exercice de leurs fonctions, conformément à la législation nationale, et par leurs autorités de coordination.

2. Le droit d'accès aux données introduites dans le SIS et le droit de les consulter directement peuvent également être exercés par les autorités judiciaires nationales, y compris celles qui sont compétentes pour engager des poursuites judiciaires dans le cadre de procédures pénales et des enquêtes judiciaires avant l'inculpation, dans l'exercice de leurs fonctions, conformément à la législation nationale, et par leurs autorités de coordination.
3. Le droit d'accès aux données introduites dans le SIS et le droit de les consulter directement peuvent être exercés par les autorités compétentes pour assumer les fonctions mentionnées au paragraphe 1, point c), dans l'exercice de ces fonctions. L'accès de ces autorités aux données est régi par le droit **national** [...].
4. Les autorités visées au présent article sont incluses dans la liste mentionnée à l'article 53, paragraphe 8.

Article 44

Autorités chargées de l'immatriculation des véhicules

1. Les services chargés, dans les États membres, de délivrer les certificats d'immatriculation des véhicules visés par la directive 1999/37/CE⁸⁷ ont accès aux données [...] introduites dans le SIS conformément à l'article 38, paragraphe 2, points a), b), c), [...] l) **et o)**, du présent règlement, exclusivement en vue de vérifier si les véhicules **à moteur, ainsi que les certificats d'immatriculation et les plaques d'immatriculation les accompagnant,** qui leur sont présentés à des fins d'immatriculation ont été volés, détournés, égarés, **sont des faux** ou sont recherchés aux fins de preuve dans une procédure pénale [...].

⁸⁷ Directive 1999/37/CE du Conseil du 29 avril 1999 relative aux documents d'immatriculation des véhicules (JO L 138 du 1.6.1999, p. 57).

[...]

[...]

[...]

L'accès à ces données par les services chargés de délivrer les certificats d'immatriculation des véhicules est régi par le droit national de chaque État membre.

2. Les services visés au paragraphe 1 qui sont des services publics ont le droit d'accéder directement aux données introduites dans le SIS.
3. Les services visés au paragraphe 1 qui ne sont pas des services publics n'ont accès aux données introduites dans le SIS que par l'intermédiaire de l'une des autorités visées à l'article 43 du présent règlement. Cette autorité a le droit d'accéder directement à ces données et de les transmettre au service concerné. L'État membre concerné veille à ce que le service en question et son personnel soient tenus de respecter toute limite fixée en ce qui concerne les conditions d'utilisation des données qui leur sont transmises par l'autorité.
4. L'article 39 du présent règlement ne s'applique pas à l'accès obtenu conformément au présent article. Toute communication à un service de police ou à une autorité judiciaire, par les services visés au paragraphe 1, d'informations apparues lors d'un accès au SIS [...] est régie par le droit national.

Article 45

Autorités chargées de l'immatriculation des bateaux et aéronefs

1. Les services chargés, dans les États membres, de délivrer les certificats d'immatriculation ou d'assurer la gestion de la circulation des bateaux, y compris des moteurs de bateaux, et des aéronefs ont accès aux données ci-après introduites dans le SIS conformément à l'article 38, paragraphe 2, du présent règlement, exclusivement en vue de vérifier si les bateaux, y compris les moteurs de bateaux, et les aéronefs, **y compris les moteurs d'aéronefs**, [...] qui leur sont présentés afin d'être immatriculés ou dans le cadre de la gestion de la circulation ont été volés, détournés ou égarés, ou sont recherchés aux fins de preuve dans une procédure pénale:

- a) les données relatives aux bateaux;
- b) les données relatives aux moteurs de bateaux;
- c) les données relatives aux aéronefs;

d) les données relatives aux moteurs d'aéronefs.

Sous réserve du paragraphe 2, l'accès de ces services à ces données est régi par la législation de chaque État membre. L'accès aux données énumérées aux points a) à **d**[...] ci-dessus est limité à la compétence spécifique des services concernés.

- 2. Les services visés au paragraphe 1 qui sont des services publics ont le droit d'accéder directement aux données introduites dans le SIS.
- 3. Les services visés au paragraphe 1 qui ne sont pas des services publics n'ont accès aux données introduites dans le SIS que par l'intermédiaire de l'une des autorités visées à l'article 43 du présent règlement. Cette autorité a le droit d'accéder directement aux données et de les transmettre au service concerné. L'État membre concerné veille à ce que le service en question et son personnel soient tenus de respecter toute limite fixée en ce qui concerne les conditions d'utilisation des données qui leur sont transmises par l'autorité.
- 4. L'article 39 du présent règlement ne s'applique pas à l'accès obtenu conformément au présent article. Toute communication à un service de police ou à une autorité judiciaire, par les services visés au paragraphe 1, d'informations apparues lors d'un accès au SIS et faisant suspecter l'existence d'une infraction pénale est régie par le droit national.

Article 45 bis

Autorités chargées de l'enregistrement des armes à feu

1. Les services chargés, dans les États membres, de délivrer les certificats d'enregistrement des armes à feu ont accès aux données relatives aux personnes faisant l'objet d'un signalement en vertu de l'article 26 ou 36 et aux données relatives aux armes à feu introduites dans le SIS conformément à l'article 38, paragraphe 2, du présent règlement afin de vérifier si la personne demandant l'enregistrement représente une menace pour la sécurité publique ou nationale ou si les armes à feu qui leur sont présentées en vue d'un enregistrement sont recherchées aux fins d'une saisie ou de la preuve dans une procédure pénale.
2. L'accès de ces services à ces données est régi par le droit national de chaque État membre⁸⁸. L'accès à ces données est limité à la compétence spécifique des services concernés.
3. Les services visés au paragraphe 1 qui sont des autorités compétentes peuvent avoir le droit d'accéder directement aux données introduites dans le SIS.
4. Les services visés au paragraphe 1 qui ne sont pas des autorités compétentes n'ont accès aux données introduites dans le SIS que par l'intermédiaire de l'une des autorités visées à l'article 43 du présent règlement. L'autorité intermédiaire a le droit d'accéder directement aux données et indique au service concerné si l'arme à feu peut ou non être enregistrée. L'État membre veille à ce que le service en question et son personnel soient tenus de respecter toute limite fixée en ce qui concerne les conditions d'utilisation des données qui leur sont transmises par l'autorité intermédiaire.
5. L'article 39 ne s'applique pas à l'accès obtenu conformément au présent article. Toute communication à un service de police ou à une autorité judiciaire, par les services visés au paragraphe 1, d'informations apparues lors d'un accès au SIS est régie par le droit national.

⁸⁸ Libellé correspondant à celui de l'article 44, paragraphe 1, dernier alinéa.

Article 46

Accès d'Europol aux données du SIS

1. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol) a, dans les limites de son mandat, le droit d'accéder aux données introduites dans le SIS et de les consulter **et peut échanger et traiter des informations supplémentaires conformément aux dispositions du manuel SIRENE mentionnées à l'article 8.**
2. Lorsqu'il ressort d'une consultation du système par Europol qu'il existe un signalement dans le SIS, Europol informe l'État membre signalant **par voie d'échange d'informations supplémentaires. Jusqu'à ce qu'Europol soit en mesure d'utiliser la fonctionnalité prévue pour l'échange d'informations supplémentaires, elle informe l'État membre signalant** par les canaux définis dans le règlement (UE) 2016/794.
- 2 bis. Europol peut traiter des informations supplémentaires qui lui ont été communiquées par les États membres à des fins de recoupement visant à établir des liens ou d'autres rapports pertinents ainsi qu'à des fins d'analyse stratégique, thématique et opérationnelle, comme le prévoit l'article 18, paragraphe 2, points a) et c), du règlement (UE) 2016/794. Tout traitement d'informations supplémentaires par Europol est réalisé conformément au règlement (UE) 2016/794.**
3. L'utilisation des informations obtenues lors d'une consultation du SIS **ou lors du traitement d'informations supplémentaires** est soumise à l'accord de l'État membre **signalant** [...]. Si ledit État membre autorise l'utilisation de ces informations, leur traitement par Europol est régi par le règlement (UE) 2016/794. Europol ne peut communiquer ces informations à des pays ou organismes tiers qu'avec le consentement de l'État membre **signalant** [...].
4. [...] ⁸⁹

⁸⁹ Conformément au règlement (UE) 2016/794, Europol peut, en tout état de cause, demander aux États membres des informations relatives aux infractions obligatoires. Le paragraphe 4 peut dès lors être considéré comme superflu.

5. Europol:

- a) sans préjudice des paragraphes 3 [...] et 6, s'abstient de connecter les parties du SIS auxquelles il a accès à un système informatisé de collecte et de traitement des données exploité par Europol ou en son sein et de transférer les données qu'elles contiennent vers un tel système, ainsi que de télécharger ou de copier, de toute autre manière, une quelconque partie du SIS;

a bis) nonobstant l'article 31, paragraphe 1, du règlement (UE) 2016/794, supprime les informations supplémentaires comportant des données à caractère personnel au plus tard un an après que le signalement correspondant a été supprimé du SIS, à moins que le maintien de la conservation des données soit jugé nécessaire, sur la base d'informations plus détaillées que celles détenues par le fournisseur des données, afin qu'Europol puisse s'acquitter de ses missions. Europol informe le fournisseur des données du maintien de la conservation de ces données, en justifiant celui-ci;

- b) limite l'accès aux données introduites dans le SIS, **y compris les informations supplémentaires**, au personnel expressément autorisé d'Europol;
- c) adopte et applique les mesures prévues aux articles 10 et 11; **et**
- d) autorise le Contrôleur européen de la protection des données à contrôler les activités qu'Europol mène dans le cadre de l'exercice de son droit d'accès aux données introduites dans le SIS et de son droit de consulter lesdites données **ainsi que dans le cadre de l'échange et du traitement d'informations supplémentaires**.

6. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire au personnel dûment autorisé d'Europol pour effectuer une consultation directe. Les dispositions du présent règlement s'appliquent à ce type de copie. La copie technique est utilisée aux fins du stockage de données du SIS pendant la consultation de ces données. Les données sont supprimées dès qu'elles ont été consultées. De telles utilisations ne sont pas considérées comme des téléchargements ou copies illicites de données du SIS. Europol s'abstient de copier des données de signalements ou des données complémentaires transmises par les États membres, ou des données provenant du CS-SIS, vers d'autres systèmes d'Europol.

7. [...]
8. [...]
9. Aux fins de vérifier la licéité du traitement des données, d'assurer un autocontrôle ainsi que de garantir la sécurité et l'intégrité des données, Europol [...] **enregistre** dans des journaux tout accès au SIS et toute consultation de celui-ci **conformément à l'article 12**. De tels journaux ne sont pas considérés comme des téléchargements ou copies illicites d'une quelconque partie du SIS.

Article 47

Accès d'Eurojust aux données du SIS

1. Les membres nationaux d'Eurojust, ainsi que leurs assistants, ont le droit, dans les limites de leur mandat, d'accéder aux données introduites dans le SIS conformément aux articles 26, 32, 34, 38 et 40 et de les consulter.
2. Lorsqu'il ressort d'une consultation du système par un membre national d'Eurojust qu'il existe un signalement dans le SIS, celui-ci en informe l'État membre signalant. **Les informations obtenues lors d'une telle consultation ne peuvent être communiquées à des pays ou instances tiers qu'avec le consentement de l'État membre signalant.**
3. Aucune disposition du présent article ne doit être interprétée comme affectant les dispositions de la décision 2002/187/JAI relatives à la protection des données et à la responsabilité du fait d'un traitement non autorisé ou incorrect de données par les membres nationaux d'Eurojust ou leurs assistants, ni comme affectant les prérogatives de l'organe de contrôle commun institué conformément à ladite décision.

4. Chaque accès aux données et chaque consultation effectuée par un membre national d'Eurojust ou un assistant est enregistré dans un journal conformément aux dispositions de l'article 12, de même que toute utilisation qu'ils ont faite des données auxquelles ils ont eu accès.
5. Aucune des parties du SIS n'est connectée à un système informatique de collecte et de traitement des données exploité par Eurojust ou en son sein, et aucune des données contenues dans le SIS auxquelles les membres nationaux ou leurs assistants ont accès n'est transférée vers un tel système informatique. Aucune partie du SIS n'est téléchargée. L'enregistrement dans un journal des accès et des consultations n'est pas considéré comme un téléchargement ou une copie illicites de données du SIS.
6. L'accès aux données introduites dans le SIS est limité aux membres nationaux et à leurs assistants et n'est pas accordé au personnel d'Eurojust.
7. Les mesures visant à garantir la sécurité et la confidentialité prévues aux articles 10 et 11 sont adoptées et appliquées.

Article 48

Accès aux données du SIS par les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents intervenant dans les tâches liées aux retours et les membres des équipes d'appui à la gestion des flux migratoires⁹⁰

1. [...] **Les membres des équipes du corps européen de garde-frontières et de garde-côtes ou des équipes d'agents intervenant dans les tâches liées aux retours, ainsi que les membres des équipes d'appui à la gestion des flux migratoires, constituées conformément aux articles 18, 20 et 32 du règlement (UE) 2016/1624, ont le droit, dans les limites de leur mandat et pour autant qu'ils soient autorisés à procéder à des vérifications conformément à l'article 43, d'accéder aux données introduites dans le SIS et de les consulter. L'accès aux données introduites dans le SIS n'est pas accordé aux membres d'autres équipes⁹¹.**

⁹⁰ Au pluriel, comme dans le règlement (UE) 2018/...

⁹¹ Texte déplacé depuis le paragraphe 5.

2. Les membres des équipes du corps européen de garde-frontières et de garde-côtes ou des équipes d'agents intervenant dans les tâches liées aux retours, ainsi que les membres des équipes d'appui à la gestion des flux migratoires, **exercent ce droit d'accéder** aux données introduites dans le SIS et de les consulter, conformément au paragraphe 1, par l'intermédiaire de l'interface technique créée et gérée par l'Agence européenne de garde-frontières et de garde-côtes telle qu'elle est prévue à l'article 49, paragraphe 1.
3. Lorsqu'il ressort d'une consultation du système par un membre des équipes du corps européen de garde-frontières et de garde-côtes, des équipes d'agents intervenant dans les tâches liées aux retours ou des équipes d'appui à la gestion des flux migratoires qu'il existe un signalement dans le SIS, l'État membre signalant en est informé. Conformément à l'article 40 du règlement (UE) 2016/1624, les membres des équipes ne peuvent agir en réaction à un signalement dans le SIS que sur les instructions et, en règle générale, en présence de garde-frontières ou d'agents intervenant dans les tâches liées au retour de l'État membre hôte dans lequel ils opèrent. L'État membre hôte peut autoriser les membres des équipes à agir en son nom.
4. Chaque accès aux données et chaque consultation effectuée par un membre des équipes du corps européen de garde-frontières et de garde-côtes, des équipes d'agents intervenant dans les tâches liées aux retours ou des équipes d'appui à la gestion des flux migratoires est enregistré dans un journal conformément aux dispositions de l'article 12, de même que toute utilisation qu'il a faite des données auxquelles il a eu accès.
5. [...] ⁹²
6. **Les équipes du corps européen de garde-frontières et de garde-côtes, les équipes d'agents intervenant dans les tâches liées aux retours ou les membres des équipes d'appui à la gestion des flux migratoires prennent les** mesures visant à garantir la sécurité et la confidentialité prévues aux articles 10 et 11 [...].

⁹² Fusionné avec le paragraphe 1.

Article 49

Accès aux données du SIS par l'Agence européenne de garde-frontières et de garde-côtes

1. Aux fins de l'article 48, paragraphe 1, [et [...] l'article **49 bis**], l'Agence européenne de garde-frontières et de garde-côtes crée et gère une interface technique permettant une connexion directe au SIS central.
- 2.⁹³ [...]
- 3.⁹⁴ [...]
4. Aucune disposition du présent article ne doit être interprétée comme affectant les dispositions du règlement (UE) 2016/1624 relatives à la protection des données et à la responsabilité du fait d'un traitement non autorisé ou incorrect de données par l'Agence européenne de garde-frontières et de garde-côtes.
5. Chaque accès aux données et chaque consultation effectuée par l'Agence européenne de garde-frontières et de garde-côtes est enregistré dans un journal conformément aux dispositions de l'article 12, de même que toute utilisation qu'elle a faite des données auxquelles elle a eu accès.
6. **Sauf dans les cas où le paragraphe 1 du présent article s'applique**, aucune des parties du SIS n'est connectée à un système informatique de collecte et de traitement des données exploité par l'Agence européenne de garde-frontières et de garde-côtes ou en son sein, et aucune des données contenues dans le SIS auxquelles cette agence a accès n'est transférée vers un tel système. Aucune partie du SIS n'est téléchargée. L'enregistrement dans un journal des accès et des consultations n'est pas considéré comme un téléchargement ou une copie de données du SIS.

⁹³ Paragraphe déplacé vers l'article 49 *bis*, paragraphe 1.

⁹⁴ Paragraphe déplacé vers l'article 49 *bis*, paragraphe 2.

7. **L'Agence européenne de garde-frontières et de garde-côte prend les** mesures visant à garantir la sécurité et la confidentialité prévues aux articles 10 et 11 [...].

[Article 49 bis]⁹⁵

Accès aux données du SIS par l'unité centrale ETIAS

1. **Pour l'accomplissement des missions que lui attribue le règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), l'Agence européenne de garde-frontières et de garde-côtes a le droit d'accéder aux données introduites dans le SIS conformément aux articles 26, 32, 34 et 36 et à l'article 38, paragraphe 2, points j) et k), et de les consulter.**
2. **Lorsqu'il ressort d'une vérification dans le système effectuée par l'Agence européenne de garde-frontières et de garde-côtes qu'il existe un signalement dans le SIS, la procédure prévue aux articles 18, 20 bis et 22 du règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) s'applique.**⁹⁶

Article 49 ter

Évaluation de l'utilisation du SIS par Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes

1. **La Commission procède, au moins tous les cinq ans, à une évaluation de l'exploitation et de l'utilisation du SIS conformément au présent règlement par Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes.**

⁹⁵ Dispositions déplacées depuis l'article 49, paragraphes 2 et 3.

⁹⁶ Le contenu et l'insertion de ces dispositions dépendent du texte final de la proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624 (voir le doc. 10017/17), et de la date de son entrée en vigueur.

2. Une équipe chargée de cette évaluation sur place est composée d'au maximum deux représentants de la Commission, assistés d'au maximum huit experts désignés par les États membres. [...]
3. La Commission établit un rapport d'évaluation après chaque évaluation, en consultant les experts désignés par les États membres. Le rapport d'évaluation est fondé sur les conclusions de l'équipe d'évaluation sur place et analyse les aspects qualitatifs, quantitatifs, opérationnels, administratifs et organisationnels de la gestion et de l'utilisation du SIS, selon ce qui convient, et recense toutes les lacunes constatées lors de l'évaluation.
4. Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes se voient chacune offrir la possibilité de formuler des observations avant l'adoption du rapport.
5. Le rapport d'évaluation est transmis au Parlement européen et au Conseil. Il est classifié EU RESTRICTED/RESTREINT UE conformément aux règles de sécurité applicables. La classification ne fait pas obstacle à que les informations soient mises à la disposition du Parlement européen.
6. À la lumière des constatations et des appréciations figurant dans le rapport d'évaluation, la Commission élabore des recommandations de mesures correctives visant à remédier à toutes les lacunes recensées au cours de l'évaluation et donne une indication des priorités pour leur mise en œuvre ainsi que, s'il y a lieu, des exemples de bonnes pratiques.
7. Après une évaluation, Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes présentent à la Commission un plan d'action visant à remédier à toutes les lacunes recensées dans le rapport d'évaluation et continuent ensuite à faire rapport tous les trois mois sur les progrès réalisés, jusqu'à ce que le plan d'action ait été intégralement mis en œuvre.

Article 50
Limites d'accès

Les utilisateurs finaux, y compris Europol, les membres nationaux d'Eurojust et leurs assistants, [...] l'Agence européenne de garde-frontières et de garde-côtes [...], **les membres des équipes du corps européen de garde-frontières et de garde-côtes ou des équipes d'agents intervenant dans les tâches liées aux retours, ainsi que les membres des équipes d'appui à la gestion des flux migratoires**, ne peuvent accéder qu'aux données qui sont nécessaires à l'accomplissement de leurs missions.

Article 51
*Durée de conservation des signalements - **personnes***⁹⁷

1. Les signalements **de personnes** introduits dans le SIS aux fins du présent règlement ne sont conservés que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits.
2. **En ce qui concerne les signalements de personnes:**
 - a) **un État membre peut introduire un signalement pour une durée de cinq ans;**
 - b) [...] l'État membre **signalant** examine, dans les cinq ans à compter de l'introduction **du** signalement dans le SIS, la nécessité de l'y maintenir. [...] ⁹⁸ [...]
3. [...]

⁹⁷ Un nouvel article 51 *bis* a été introduit pour régir la durée de conservation des signalements d'objets.

⁹⁸ Déplacé vers le paragraphe 3.

Par dérogation au paragraphe 2, en ce qui concerne les signalements introduits aux fins de l'article 32, paragraphe 2, points c) et d), et de l'article 36 du présent règlement⁹⁹:

a) un État membre peut introduire un signalement pour une durée d'un an;

b) l'État membre signalant examine, dans un délai d'un an à compter de l'introduction du signalement dans le SIS, la nécessité de l'y maintenir.

4. Chaque État membre fixe, s'il y a lieu, des délais d'examen plus courts, conformément à son droit national.

5. **L'État membre signalant peut, dans le délai d'examen, décider, au terme d'une évaluation individuelle globale, qui est enregistrée, de maintenir le signalement d'une personne si les fins auxquelles le signalement a été effectué l'exigent. Dans ce cas, le paragraphe 2, point a), ou le paragraphe 3, point a), s'applique également à la prolongation du signalement. Toute prolongation d'un signalement est communiquée au CS-SIS¹⁰⁰.**

[...] ¹⁰¹

⁹⁹ Texte en partie déplacé depuis le paragraphe 2.

¹⁰⁰ Déplacé depuis le paragraphe 6.

¹⁰¹ Déplacé vers le paragraphe 8.

6. [...] ¹⁰²

Les signalements sont automatiquement [...] **supprimés** à l'expiration du délai d'examen visé au paragraphe 2, **point b), et au paragraphe 3, point b)**, sauf dans le cas où l'État membre signalant a informé le CS-SIS de la prolongation du signalement **d'une personne** conformément au paragraphe **5**. Le CS-SIS informe automatiquement les États membres de la suppression programmée de données dans le système moyennant un préavis de quatre mois¹⁰³.

7. [...] ¹⁰⁴

Les États membres tiennent des statistiques concernant le nombre de signalements **de personnes** dont la durée de conservation a été prolongée conformément au paragraphe [...] **5**¹⁰⁵.

8. [...] ¹⁰⁶

¹⁰² Déplacé vers le paragraphe 5.

¹⁰³ Déplacé depuis le paragraphe 7.

¹⁰⁴ Déplacé vers le paragraphe 6.

¹⁰⁵ Déplacé depuis le paragraphe 8.

¹⁰⁶ Déplacé vers le paragraphe 7.

Lorsqu'il est clair pour le personnel du bureau SIRENE, chargé de coordonner et de vérifier la qualité des données, que le signalement d'une personne a atteint son objectif et devrait être supprimé du SIS, ce personnel **porte la question à l'attention de** [...] l'autorité signalante [...]. L'autorité dispose d'un délai de 30 jours civils à compter de la réception de cette notification pour indiquer que le signalement a été ou sera supprimé ou pour exposer les raisons du maintien du signalement. Faute de réponse à l'expiration du délai de 30 jours, le personnel du bureau SIRENE, **si le droit national l'y autorise**, supprime le signalement. Les bureaux SIRENE signalent tout problème récurrent dans ce domaine à leur autorité de contrôle nationale¹⁰⁷.

Article 51 bis

Durée de conservation des signalements - objets¹⁰⁸

- 1. Les signalements introduits dans le SIS aux fins du présent règlement qui concernent des objets ne sont conservés que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits.**
- 2. En ce qui concerne les signalements d'objets:**
 - a) **un État membre peut introduire un signalement concernant des objets pour une durée de dix ans;**
 - b) **un État membre peut introduire un signalement concernant d'autres objets conformément aux articles 26, 32, 34, 36 et 38 pour une durée de cinq ans s'ils sont liés à des signalements de personnes;**
 - c) **les délais de conservation visés aux points a) et b) du présent paragraphe peuvent être prolongés si les fins auxquelles le signalement a été effectué l'exigent. Dans ce cas, les points a) et b) du présent paragraphe s'appliquent également à la prolongation;**
 - d) **des durées de conservation plus brèves peuvent être établies pour des catégories de signalements d'objets au moyen de mesures d'exécution adoptées conformément à la procédure d'examen visée à l'article 72, paragraphe 2.**

¹⁰⁷ Déplacé depuis le paragraphe 5.

¹⁰⁸ Ce nouvel article porte spécifiquement sur la durée de conservation des signalements d'objets et reproduit, mutatis mutandis, les dispositions relatives à la durée de conservation des signalements de personnes (article 51).

3. **Les États membres tiennent des statistiques concernant le nombre de signalements d'objets dont la durée de conservation a été prolongée conformément au paragraphe 2, point c).**

CHAPITRE XIII SUPPRESSION DES SIGNALEMENTS

Article 52

Suppression des signalements

1. La suppression de signalements effectués en vertu de l'article 26 en vue d'une arrestation aux fins de remise ou d'extradition a lieu lorsque la personne a été remise aux autorités compétentes de l'État membre signalant ou extradée vers celui-ci. Elle **se produit** [...] également lorsque la décision judiciaire sur laquelle reposait le signalement a été révoquée par l'autorité judiciaire compétente conformément au droit national.
2. La suppression des signalements de personnes disparues, **d'enfants risquant d'être enlevés ou de personnes vulnérables introduits conformément à l'article 32** obéit aux règles suivantes:
 - a) en ce qui concerne les enfants disparus [...] **et les enfants risquant d'être enlevés** [...], le signalement est supprimé:
 - dès la résolution de l'affaire, par exemple lorsque l'enfant a été rapatrié ou lorsque les autorités compétentes de l'État membre d'exécution ont arrêté une décision relative à la prise en charge de l'enfant;
 - dès l'expiration du signalement conformément à l'article 51;
 - dès l'adoption d'une décision par l'autorité compétente de l'État membre signalant; ou
 - [...]
 - **lorsque le risque d'enlèvement a disparu;**

- b) en ce qui concerne les adultes disparus [...], lorsqu'aucune mesure de protection n'est demandée, le signalement est supprimé:
- dès l'exécution de la conduite à tenir (lieu de séjour constaté par l'État membre d'exécution);
 - dès l'expiration du signalement conformément à l'article 51; ou
 - dès l'adoption d'une décision par l'autorité compétente de l'État membre signalant;
- c) en ce qui concerne les adultes disparus [...], lorsque des mesures de protection sont demandées, le signalement est supprimé:
- dès l'exécution de la conduite à tenir (personne placée sous protection);
 - dès l'expiration du signalement conformément à l'article 51; ou
 - dès l'adoption d'une décision par l'autorité compétente de l'État membre signalant;
- d) en ce qui concerne les personnes vulnérables qui doivent être empêchées de voyager pour leur propre protection, le signalement est supprimé:**
- **dès l'exécution de la conduite à tenir (personne placée sous protection);**
 - **dès l'expiration du signalement conformément à l'article 51; ou**
 - **dès l'adoption d'une décision par l'autorité compétente de l'État membre signalant¹⁰⁹.**

Sous réserve des dispositions du droit national, lorsqu'une personne a été internée sur décision d'une autorité compétente, le signalement peut être maintenu jusqu'au rapatriement de cette personne.

¹⁰⁹ Texte similaire à celui du point c).

3. [...] En ce qui concerne les personnes recherchées dans le cadre d'une procédure judiciaire au sens de l'article 34, le signalement est supprimé:

- a) dès la communication du lieu de séjour de la personne à l'autorité compétente de l'État membre signalant. Lorsqu'aucune suite ne peut être donnée aux informations transmises, le bureau SIRENE de l'État membre signalant informe son homologue de l'État membre d'exécution afin de résoudre le problème;
- b) dès l'expiration du signalement conformément à l'article 51; ou
- c) dès l'adoption d'une décision par l'autorité compétente de l'État membre signalant.

Lorsqu'une réponse positive a été obtenue dans un État membre et que l'adresse a été communiquée à l'État membre signalant et qu'une autre réponse positive dans cet État membre révèle la même adresse, le signalement est enregistré [...] dans l'État membre d'exécution mais ni l'adresse ni les informations supplémentaires ne doivent être renvoyées à l'État membre signalant. En pareil cas, l'État membre d'exécution informe l'État membre signalant de ces réponses positives répétées et ce dernier évalue la nécessité de maintenir le signalement.

4. [...] En ce qui concerne les signalements concernant des contrôles discrets, d'investigation ou spécifiques au sens de l'article 36, le signalement est supprimé:

- a) dès l'expiration du signalement conformément à l'article 51;
- b) dès l'adoption d'une décision de suppression par l'autorité compétente de l'État membre signalant.

5. [...] En ce qui concerne les signalements d'objets introduits aux fins d'une saisie ou de la preuve au sens de l'article 38, le signalement est supprimé:
- a) dès la saisie de l'objet ou mesure équivalente, lorsque le nécessaire échange consécutif d'informations supplémentaires a eu lieu entre les bureaux SIRENE ou que l'objet est désormais visé par une autre procédure judiciaire ou administrative;
 - b) dès l'expiration du signalement; ou
 - c) dès l'adoption d'une décision de suppression par l'autorité compétente de l'État membre signalant.
6. Les signalements de personnes recherchées inconnues au sens de l'article 40 sont supprimés:
- [...] a) dès l'identification de la personne; ou
 - [...] b) dès l'expiration du signalement.

CHAPITRE XIV

RÈGLES GÉNÉRALES RELATIVES AU TRAITEMENT DES DONNÉES

Article 53

Traitement des données du SIS

1. Les États membres ne peuvent traiter les données visées à l'article 20 qu'aux fins énoncées pour chacune des catégories de signalements visées aux articles 26, 32, 34, 36, 38 et 40.
2. Les données ne peuvent être copiées qu'à des fins techniques, pour autant que cette copie soit nécessaire aux autorités visées à l'article 43 pour effectuer une consultation directe **ou à l'agence eu-Lisa pour assurer la disponibilité continue du SIS central.** Les dispositions du présent règlement s'appliquent à ce type de copie. Tout État membre s'abstient de copier des données de signalements ou des données complémentaires saisies par un autre État membre, de son N.SIS ou du CS-SIS vers d'autres fichiers de données nationaux.
3. Les copies techniques visées au paragraphe 2 alimentant des bases de données hors ligne ne peuvent être conservées que pour une durée inférieure à 48 heures. Cette durée peut être prolongée dans une situation d'urgence jusqu'à ce que cette situation d'urgence prenne fin.
4. Les États membres tiennent à jour un inventaire de ces copies, le mettent à la disposition de leur autorité de contrôle nationale et veillent à ce que ces copies soient conformes aux dispositions du présent règlement, et notamment celles de l'article 10.
5. L'accès aux données est autorisé uniquement dans les limites des compétences des autorités nationales visées à l'article 43 et réservé au personnel dûment autorisé.

6. En ce qui concerne les signalements prévus aux articles 26, 32, 34, 36, 38 et 40 du présent règlement, tout traitement des informations qui figurent dans le SIS à des fins autres que celles pour lesquelles elles y ont été introduites doit se rapporter à un cas précis et être justifié par la nécessité de prévenir une menace grave imminente pour l'ordre et la sécurité publics, pour des raisons graves de sécurité nationale ou aux fins de la prévention d'une infraction grave. À cet effet, l'autorisation préalable de l'État membre signalant doit être obtenue.
7. Toute utilisation de données non conforme aux paragraphes 1 à 6 est considérée comme un détournement de finalité au regard du droit national de chaque État membre.
8. Chaque État membre communique à l'agence eu-LISA la liste de ses autorités compétentes autorisées à consulter directement les données introduites dans le SIS en application du présent règlement, ainsi que tout changement apporté à cette liste. La liste indique, pour chaque autorité, les données qu'elle peut consulter et à quelles fins. L'agence eu-LISA veille à ce que la liste soit publiée chaque année au *Journal officiel de l'Union européenne*.
9. Pour autant que le droit de l'Union ne prévoit pas de dispositions particulières, le droit de chaque État membre est applicable aux données introduites dans son N.SIS.

Article 54

Données du SIS et fichiers nationaux

1. L'article 53, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver, dans ses fichiers nationaux, des données du SIS sur la base desquelles la conduite à tenir a été exécutée sur son territoire. Ces données sont conservées dans les fichiers nationaux pour une durée maximale de trois ans, sauf si des dispositions particulières du droit national prévoient une durée de conservation plus longue.
2. L'article 53, paragraphe 2, n'affecte pas le droit qu'a un État membre de conserver, dans ses fichiers nationaux, des données contenues dans un signalement particulier qu'il a lui-même introduit dans le SIS.

Article 55

Information en cas d'inexécution de la conduite à tenir demandée dans un signalement

Si une conduite à tenir demandée ne peut être exécutée, l'État membre requis en informe directement l'État membre signalant [...] **par voie d'échange d'informations supplémentaires.**

Article 56

Qualité des données traitées dans le SIS

1. Un État membre signalant est responsable de l'exactitude et de l'actualité des données, ainsi que de la licéité de leur introduction dans le SIS.
2. Seul l'État membre signalant est autorisé à modifier, compléter, rectifier, mettre à jour ou supprimer les données qu'il a introduites.
3. Lorsqu'un État membre autre que l'État membre signalant dispose d'indices faisant présumer qu'une donnée est matériellement erronée ou a été stockée illégalement, il en informe l'État membre signalant, par voie d'échange d'informations supplémentaires, dans les meilleurs délais et au plus tard dix jours après avoir relevé ces indices. L'État membre signalant vérifie ce qui lui est communiqué et, s'il y a lieu, corrige ou supprime la donnée sans délai.
4. Si les États membres ne peuvent parvenir à un accord dans un délai de deux mois à compter de la découverte des indices, tels qu'ils sont décrits au paragraphe 3, l'État membre qui n'est pas à l'origine du signalement soumet la question **au Contrôleur européen de la protection des données qui, en coopération avec les** autorités de contrôle nationales concernées [...], **agit en tant que médiateur**¹¹⁰.

¹¹⁰ Texte inspiré de celui de l'article 49, paragraphe 4, de la décision 2007/533/JAI.

5. Les États membres échangent des informations supplémentaires lorsqu'une personne se plaint de ne pas être celle visée par un signalement. Lorsqu'il ressort des vérifications qu'il existe effectivement deux personnes différentes, la personne qui s'est plainte est informée des mesures établies à l'article 59.
6. Lorsqu'une personne fait déjà l'objet d'un signalement dans le SIS, l'État membre qui introduit un nouveau signalement **vérifie la compatibilité des signalements, respecte leur priorité et, si nécessaire, échange des informations supplémentaires** [...].

Article 57

Incidents de sécurité

1. Tout événement ayant ou pouvant avoir un impact sur la sécurité du SIS [...] **ou** susceptible de causer aux données de celui-ci **ou aux informations supplémentaires** des dommages ou des pertes est considéré comme un incident de sécurité, en particulier lorsque des données peuvent avoir été consultées sans autorisation ou que la disponibilité, l'intégrité et la confidentialité de données ont été ou peuvent avoir été compromises.
2. Les incidents de sécurité sont gérés de telle sorte qu'une réponse rapide, efficace et idoine y soit apportée.
3. Les États membres, **Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes** informent la Commission, l'agence eu-LISA et l'autorité de contrôle nationale des incidents de sécurité. L'agence eu-LISA informe la Commission et le Contrôleur européen de la protection des données des incidents de sécurité.
4. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement du SIS dans un État membre ou au sein de l'agence eu-LISA, ou sur la disponibilité, l'intégrité et la confidentialité des données saisies ou envoyées par d'autres États membres **ou des informations supplémentaires échangées**, sont communiquées **à tous les** États membres et signalées conformément au plan de gestion des incidents fourni par l'agence eu-LISA.

Article 58

Différenciation des personnes présentant des caractéristiques similaires

Si, lors de l'introduction d'un nouveau signalement, il apparaît qu'il existe déjà dans le SIS une personne correspondant à la même description, la procédure ci-après s'applique:

- b) a) le bureau SIRENE prend contact avec le service demandeur pour vérifier s'il s'agit ou non de la même personne; **et**

- c) b) lorsque la vérification fait apparaître que la personne faisant l'objet du nouveau signalement et la personne déjà signalée dans le SIS sont bien une seule et même personne, le bureau SIRENE applique la procédure concernant les signalements multiples visée à l'article 56, paragraphe 6. Lorsque la vérification révèle qu'il s'agit en réalité de deux personnes différentes, le bureau SIRENE valide la demande d'introduction du deuxième signalement, en ajoutant les éléments nécessaires pour éviter toute erreur d'identification.

Article 59

Données complémentaires pour traiter les cas d'usurpation d'identité

1. Lorsqu'il est possible de confondre la personne effectivement visée par un signalement et une personne dont l'identité a été usurpée, l'État membre signalant ajoute dans le signalement, avec le consentement explicite de la personne dont l'identité a été usurpée, des données concernant cette dernière afin d'éviter les effets négatifs résultant d'une erreur d'identification.

2. Les données concernant une personne dont l'identité a été usurpée sont exclusivement utilisées pour:
 - a) permettre aux autorités compétentes de distinguer la personne dont l'identité a été usurpée de la personne effectivement visée par le signalement;

 - b) permettre à la personne dont l'identité a été usurpée de prouver son identité et d'établir que celle-ci a été usurpée.

3. Aux fins du présent article, seules les données à caractère personnel ci-après **de la personne dont l'identité a été usurpée** peuvent être introduites dans le SIS et faire l'objet d'un traitement ultérieur:

- a) le[...]s nom[...]s;
- b) le[...]s prénom[...]s;
- a) le[...]s nom[...]s à la naissance;
- b) les noms utilisés antérieurement ainsi que les pseudonymes éventuellement enregistrés séparément;
- c) les signes physiques particuliers, objectifs et inaltérables;
- d) le lieu de naissance;
- e) la date de naissance;
- f) le [...] **genre**;
- g) les photographies et les images faciales;
- h) les [...] **données dactyloscopiques**;
- i) la [...] nationalité/**les nationalités**;
- j) la catégorie **des documents d'identification** [...] de la personne;
- k) le pays de délivrance **des documents d'identification** [...] de la personne;
- l) le(s) numéro(s) **des documents d'identification** [...] de la personne;
- m) la date de délivrance **des documents d'identification** [...] de la personne;
- n) l'adresse de la **personne** [...];
- o) le nom du père de la **personne** [...];
- p) le nom de la mère de la **personne** [...].

4. Les règles techniques nécessaires pour l'introduction et pour le traitement ultérieur des données mentionnées au paragraphe 3 sont établies au moyen de mesures d'exécution définies et précisées conformément à la procédure d'examen visée à l'article 72, paragraphe 2.
5. Les données mentionnées au paragraphe 3 sont supprimées en même temps que le signalement correspondant, ou plus tôt lorsque la personne concernée le demande.
6. Seules les autorités disposant d'un droit d'accès au signalement correspondant peuvent accéder aux données mentionnées au paragraphe 3, et ce dans l'unique but d'éviter une erreur d'identification.

Article 60

Mise en relation de signalements

1. Un État membre peut mettre en relation des signalements qu'il introduit dans le SIS. Cette mise en relation a pour effet d'établir un lien entre deux ou plusieurs signalements.
2. La mise en relation est sans effet sur la conduite particulière à tenir qui est demandée dans chacun des signalements mis en relation, ou sur leur durée de conservation.
3. La mise en relation ne porte pas atteinte aux droits d'accès prévus par le présent règlement. Les autorités ne disposant pas d'un droit d'accès à certaines catégories de signalements ne doivent pas pouvoir prendre connaissance du lien vers un signalement auquel elles n'ont pas accès.
4. Un État membre met en relation des signalements lorsque cela répond à un besoin opérationnel.
5. Lorsqu'un État membre estime que la mise en relation de signalements par un autre État membre n'est pas compatible avec son droit national ou ses obligations internationales, il peut prendre les mesures nécessaires pour faire en sorte que le lien établi ne soit pas accessible à partir de son territoire national ou pour les autorités relevant de sa juridiction établies en dehors de son territoire.
6. Les règles techniques nécessaires pour la mise en relation des signalements sont établies et précisées conformément à la procédure d'examen visée à l'article 72, paragraphe 2.

Article 61

Objet et durée de conservation des informations supplémentaires

1. Les États membres conservent au sein du bureau SIRENE une trace des décisions ayant donné lieu à un signalement, afin de faciliter l'échange d'informations supplémentaires.
2. Les données à caractère personnel conservées au sein du bureau SIRENE à la suite d'un échange d'informations ne sont conservées que pendant le temps nécessaire à la réalisation des objectifs pour lesquels elles ont été fournies. Elles sont, en tout état de cause, supprimées au plus tard un an après que le signalement correspondant a été supprimé du SIS.
3. Le paragraphe 2 n'affecte pas le droit qu'a un État membre de conserver, dans des fichiers nationaux, des données relatives à un signalement particulier que cet État membre a introduit dans le SIS ou à un signalement sur la base duquel une conduite à tenir demandée a été exécutée sur son territoire. Le délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par la législation nationale.

Article 62

Transfert de données à caractère personnel à des tiers

Les données traitées dans le SIS et les informations supplémentaires connexes au titre du présent règlement ne sont pas transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition.

Article 63

[...]

[...]

CHAPITRE XV PROTECTION DES DONNÉES

Article 64

Législation applicable

1. Le règlement (CE) n° 45/2001 s'applique aux traitements de données à caractère personnel effectués par l'agence eu-LISA **et par l'Agence européenne de garde-frontières et de garde-côtes** au titre du présent règlement. **Le règlement (UE) 2016/794 (règlement Europol) s'applique au traitement de données à caractère personnel effectué par Europol au titre du présent règlement. La décision 2002/187/JAI (Eurojust) s'applique au traitement de données à caractère personnel effectué par Eurojust au titre du présent règlement.**
2. Le règlement (UE) 2016/679 s'applique aux traitements de données à caractère personnel pour autant que
[...] la directive (UE) 2016/680 ne s'applique pas.

3. **Les dispositions nationales transposant la directive (UE) 2016/680 s'appliquent aux** [...] traitements de données effectués par les autorités nationales compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces [...].

Article 65

Droit d'accès, de rectification des données inexactes et d'effacement de données stockées illégalement

1. Le droit de toute personne concernée d'accéder aux données la concernant qui sont introduites dans le SIS et de faire rectifier ou effacer ces données s'exerce dans le respect de la législation de l'État membre auprès duquel elle fait valoir ce droit.
2. [...]
3. Un État membre autre que celui qui a introduit le signalement ne peut communiquer des informations concernant ces données **à une personne concernée** que [...] **si chaque** État membre signalant [...] **donne son accord**. Cela se fait par voie d'échange d'informations supplémentaires.
4. Un État membre peut décider de ne pas communiquer des informations à la personne concernée, en tout ou en partie, conformément au droit national, dès lors et aussi longtemps qu'une restriction partielle ou complète de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne [...] concernée, pour:

- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
 - b) éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales;
 - c) protéger la sécurité publique;
 - d) protéger la sécurité nationale; **ou**
 - e) protéger les droits et libertés d'autrui.
5. [...]
6. [...] **À la suite d'une demande d'accès, de rectification ou d'effacement, la personne concernée** est informée, dans les meilleurs délais [...] après la date [...] de la demande, **de la suite donnée à l'exercice de ces droits**¹¹¹.
7. [...]¹¹²

Article 66

Voies de recours

1. Toute personne peut saisir les juridictions ou **toute** [...] autorité compétente en vertu du droit national [...] pour consulter, faire rectifier ou effacer des données ou obtenir des informations ou pour obtenir une indemnisation en raison d'un signalement la concernant.

¹¹¹ Paragraphe fusionné avec le paragraphe 7.

¹¹² Fusionné avec le paragraphe 6.

2. Les États membres s'engagent mutuellement à exécuter les décisions définitives rendues par les juridictions ou autorités visées au paragraphe 1, sans préjudice des dispositions de l'article 70.
3. [...] **L**es autorités nationales [...] **font** rapport annuellement sur:
- a) le nombre de demandes d'accès présentées par des personnes concernées au responsable du traitement et le nombre de cas où l'accès aux données a été accordé;
 - b) le nombre de demandes d'accès présentées par des personnes concernées à l'autorité de contrôle nationale et le nombre de cas où l'accès aux données a été accordé;
 - c) le nombre de demandes de rectification de données inexactes et d'effacement de données stockées illégalement présentées au responsable du traitement et le nombre de cas où les données ont été rectifiées ou effacées;
 - d) le nombre de demandes de rectification de données inexactes et d'effacement de données stockées illégalement présentées à l'autorité de contrôle nationale;
 - e) le nombre d'affaires **dans lesquelles une décision de justice définitive a été rendue**¹¹³ [...];
- [...] ¹¹⁴[...]; **et**
- g) toute observation relative aux cas de reconnaissance mutuelle de décisions définitives rendues par les juridictions ou les autorités d'autres États membres concernant des signalements créés par un État membre signalant.

Les rapports des autorités de contrôle nationales sont transmis par l'intermédiaire du mécanisme de coopération établi à l'article 69.

¹¹³ Texte provenant du point f).

¹¹⁴ Fusionné avec le point e).

Article 67

Contrôle du N.SIS

1. Chaque État membre veille à ce que l'autorité [...] de contrôle nationale désignée dans chaque État membre et investie des pouvoirs mentionnés au chapitre VI de la directive (UE) 2016/680 ou au chapitre VI du règlement (UE) 2016/679 contrôle en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS sur son territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires **sur son territoire.**
2. L'autorité de contrôle nationale veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données dans le cadre de son N.SIS, répondant aux normes internationales en matière d'audit. Soit l'audit est effectué par l'autorité de contrôle nationale, soit cette autorité commande directement l'audit à un auditeur indépendant en matière de protection des données. En toutes circonstances, l'autorité de contrôle nationale conserve le contrôle de l'auditeur indépendant et assume la responsabilité des travaux de celui-ci.
3. Les États membres veillent à ce que l'autorité de contrôle nationale dispose des ressources nécessaires pour s'acquitter des tâches qui lui sont confiées par le présent règlement.

Article 68

Contrôle de l'agence eu-LISA

1. Le Contrôleur européen de la protection des données veille à ce que les activités de traitement des données à caractère personnel exercées par l'agence eu-LISA soient effectuées conformément au présent règlement. Les fonctions et les compétences énumérées aux articles 46 et 47 du règlement (CE) n° 45/2001 s'appliquent en conséquence.

2. Le Contrôleur européen de la protection des données [...] **réalise**, tous les quatre ans au minimum, un audit des activités de traitement des données à caractère personnel exercées par l'agence eu-LISA, répondant aux normes internationales d'audit. Un rapport d'audit est communiqué au Parlement européen, au Conseil, à l'agence eu-LISA, à la Commission et aux autorités de contrôle nationales. L'agence eu-LISA se voit offrir la possibilité de formuler des observations avant l'adoption du rapport.

Article 69

Coopération entre les autorités nationales de contrôle et le Contrôleur européen de la protection des données

1. Les autorités de contrôle nationales et le Contrôleur européen de la protection des données, agissant chacun dans les limites de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités et assurent un contrôle coordonné du SIS.
2. Agissant chacun dans les limites de leurs compétences respectives, ils échangent les informations utiles, s'assistent mutuellement pour mener les audits et inspections, examinent les difficultés d'interprétation ou d'application du présent règlement ou d'autres actes juridiques applicables de l'Union, étudient les problèmes révélés lors de l'exercice du contrôle indépendant ou de l'exercice des droits de la personne concernée, formulent des propositions harmonisées de solutions communes aux éventuels problèmes et assurent la sensibilisation aux droits en matière de protection des données, selon les besoins.
3. Aux fins énoncées au paragraphe 2, les autorités de contrôle nationales et le Contrôleur européen de la protection des données se réunissent au minimum deux fois par an, dans le cadre du comité européen de la protection des données établi par le règlement (UE) 2016/679. [...] Le règlement intérieur est adopté lors de la première réunion. D'autres méthodes de travail sont mises au point d'un commun accord, selon les besoins.
4. Un rapport d'activités conjoint relatif au contrôle coordonné est transmis [...] **annuellement** par le comité établi par le règlement (UE) 2016/679 au Parlement européen, au Conseil et à la Commission.

CHAPITRE XVI
RESPONSABILITÉ ET SANCTIONS¹¹⁵

Article 70

Responsabilité

1. Chaque État membre est responsable, **conformément au droit national**, de tout dommage causé à une personne du fait de l'exploitation du N.SIS. Il en va de même en cas de dommage causé par l'État membre signalant, lorsque ce dernier a introduit des données matériellement erronées ou a stocké des données de manière illicite.
2. Lorsque l'État membre contre lequel une action est intentée n'est pas l'État membre signalant, ce dernier est tenu de rembourser, sur demande, les sommes versées à titre d'indemnisation, à moins que l'utilisation des données par l'État membre demandant le remboursement soit contraire au présent règlement.
3. Lorsque le non-respect, par un État membre, des obligations qui lui incombent en vertu du présent règlement entraîne un dommage pour le SIS, cet État membre en est tenu responsable, sauf si et dans la mesure où l'agence eu-LISA ou [...] **d'autres États membres** participant au SIS n'ont pas pris de mesures raisonnables pour empêcher la survenance du dommage ou pour en atténuer l'effet.

Article 70 bis

Sanctions¹¹⁶

Les États membres veillent à ce que toute utilisation frauduleuse de données introduites dans le SIS ou tout échange d'informations supplémentaires contraire au présent règlement fasse l'objet de sanctions effectives, proportionnées et dissuasives conformément à leur droit national.

¹¹⁵ Les termes "et sanctions" ont été ajoutés en raison de l'insertion d'un nouvel article 53 *bis* / 70 *bis*.

¹¹⁶ Nouvel article, similaire à l'article 65 de la décision 2007/533/JAI.

CHAPITRE XVII

DISPOSITIONS FINALES

Article 71

Suivi et statistiques

1. L'agence eu-LISA veille à ce que des procédures soient mises en place pour assurer le suivi du fonctionnement du SIS par rapport aux objectifs fixés, tant en termes de résultats que de rapport coût-efficacité, de sécurité et de qualité de service.
2. Aux fins de la maintenance technique et de l'établissement de rapports, **de rapports sur la qualité des données** et de statistiques, l'agence eu-LISA a accès aux informations nécessaires concernant les opérations de traitement effectuées dans le SIS central.
3. L'agence eu-LISA publie des statistiques journalières, mensuelles et annuelles, présentant le nombre d'enregistrements par catégorie de signalements, **sous forme de totaux et ventilées par État membre. L'agence eu-LISA établit également des rapports** sur le nombre de réponses positives par catégorie de signalements, le nombre de fois où le SIS a été consulté et où on a eu accès au système pour introduire, actualiser ou supprimer un signalement, sous forme de totaux et ventilés par État membre. Les statistiques ne contiennent pas de données à caractère personnel. Le rapport statistique annuel est publié. L'agence eu-LISA fournit également des statistiques annuelles sur l'utilisation de la fonctionnalité permettant de rendre temporairement non consultable un signalement introduit en [...] **application** de l'article 26 du présent règlement, sous forme de totaux et ventilées par État membre, y compris sur toute prolongation de la durée **initiale** de non-disponibilité de 48 heures.
4. Les États membres ainsi qu'Europol, Eurojust et l'Agence européenne de garde-frontières et de garde-côtes communiquent à l'agence eu-LISA et à la Commission les informations nécessaires pour établir les rapports visés aux paragraphes 3, **5**, 7 et 8¹¹⁷.

¹¹⁷ Texte déplacé vers le paragraphe 4 *bis*.

- 4 bis.**¹¹⁸ Ces informations comprennent des statistiques distinctes sur le nombre de consultations effectuées par ou pour les services chargés, dans les États membres, de l'immatriculation des véhicules ainsi que les services chargés, dans les États membres, de délivrer les certificats d'immatriculation ou d'assurer la gestion de la circulation des bateaux, y compris les moteurs de bateaux, **et des aéronefs, y compris les moteurs d'aéronefs** [...]. Les statistiques présentent également le nombre de réponses positives par catégorie de signalements.
5. L'agence eu-LISA communique aux États membres, à la Commission, à Europol, à Eurojust et à l'Agence européenne de garde-frontières et de garde-côtes tout rapport statistique qu'elle produit. Pour contrôler la mise en œuvre des actes juridiques de l'Union, **en particulier le règlement (UE) n° 1053/2013 du Conseil**¹¹⁹, la Commission peut demander à l'agence eu-LISA de fournir d'autres rapports statistiques spécifiques, réguliers ou ponctuels, sur la performance ou l'utilisation du SIS **central** et sur [...] **l'échange d'informations supplémentaires**.
6. Aux fins des paragraphes 3, 4 [...] **ou** 5 du présent article et de l'article 15, paragraphe 5, l'agence eu-LISA crée, met en œuvre et héberge un fichier central sur ses sites techniques contenant les [...] **rapports** mentionnés au paragraphe 3 du présent article et à l'article 15, paragraphe 5, qui ne permette pas l'identification des individus mais permette à la Commission et aux agences mentionnées au paragraphe 5 d'obtenir des rapports et statistiques sur mesure. L'agence eu-LISA accorde aux États membres, à la Commission, à Europol, à Eurojust et à l'Agence européenne de garde-frontières et de garde-côtes un accès au fichier central, au moyen d'un accès sécurisé via l'infrastructure de communication, assorti d'un contrôle d'accès et de profils d'utilisateurs spécifiques aux seules fins de l'établissement de rapports et de statistiques¹²⁰.

¹¹⁸ Déplacé depuis le paragraphe 4.

¹¹⁹ Règlement (UE) n° 1053/2013 du Conseil du 7 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen et abrogeant la décision du comité exécutif du 16 septembre 1998 concernant la création d'une commission permanente d'évaluation et d'application de Schengen (JO L 295 du 6.11.2013, p. 27).

¹²⁰ Texte déplacé vers le paragraphe 9.

[...]7. [...] **T**ous les deux ans, l'agence eu-LISA présente au Parlement européen et au Conseil un rapport sur le fonctionnement technique du SIS central et de l'infrastructure de communication, y compris la sécurité offerte, et sur les échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres.

8. [...] **T**ous les quatre ans, la Commission présente un rapport d'évaluation globale du SIS central et des échanges bilatéraux et multilatéraux d'informations supplémentaires entre les États membres. Cette évaluation globale comprend un examen des résultats obtenus au regard des objectifs fixés, détermine si les principes de base restent valables, fait le point sur l'application du présent règlement en ce qui concerne le SIS central et sur la sécurité offerte par le SIS central et en tire toutes les conséquences pour le fonctionnement futur. La Commission transmet le rapport d'évaluation au Parlement européen et au Conseil.

9.¹²¹ La Commission adopte des actes d'exécution pour établir et préciser les modalités de fonctionnement du fichier central **visé au paragraphe 6** et les règles de sécurité applicables **à ce fichier. Ces actes** d'exécution **sont** adoptés en conformité avec la procédure d'examen visée à l'article 72, paragraphe 2.

Article 72

Procédure de comité

1. La Commission est assistée par un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

¹²¹ Texte déplacé depuis le paragraphe 6 in fine.

Article 73

[...]

[...] ¹²² [...] * [...] **

[...] *

[...] **

[...] ¹²³

Article 74

Abrogation

Dès la date d'application du présent règlement, les actes juridiques ci-après sont abrogés:

règlement (CE) n° 1986/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II);

¹²² [...]

¹²³ Article supprimé, car le présent instrument ne modifie pas le règlement (UE) n° 515/2014.

décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II);

décision 2010/261/UE de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication¹²⁴.

Article 75

Entrée en vigueur et applicabilité

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
2. Il s'applique à partir de la date fixée par la Commission après que:
 - a) les mesures d'application nécessaires ont été adoptées;
 - b) les États membres ont informé la Commission qu'ils ont pris les dispositions techniques et juridiques nécessaires pour traiter les données du SIS et échanger des informations supplémentaires en vertu du présent règlement;
 - c) l'agence eu-LISA a informé la Commission de l'achèvement **concluant** de toutes les activités de test concernant le CS-SIS et l'interaction entre le CS-SIS et les N.SIS.

[...] Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités [...].

¹²⁴ Décision 2010/261/UE de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication (JO L 112 du 5.5.2010, p. 31).