COMMISSION
EUROPÉENNE

Bruxelles, le 6.4.2016
COM(2016) 205 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité

1. INTRODUCTION

L'Europe est un espace caractérisé par la mobilité. Des millions de citoyens de l'Union et de ressortissants de pays tiers franchissent chaque jour les frontières intérieures et extérieures de l'UE. En 2015, plus de 50 millions de ressortissants de pays tiers se sont rendus dans l'UE, ce qui représente plus de 200 millions de franchissements des frontières extérieures de l'espace Schengen.

Outre ces flux de voyageurs en règle, le conflit syrien et les crises ailleurs dans le monde ont entraîné, pour la seule année 2015, 1,8 million de franchissements irréguliers des frontières extérieures de l'Europe. Les citoyens de l'Union attendent un contrôle efficace des personnes aux frontières extérieures, qui permette une bonne gestion des migrations et contribue à la sécurité intérieure. Les attentats terroristes perpétrés à Paris en 2015 et à Bruxelles en mars 2016 ont cruellement mis en évidence la réalité de la menace qui pèse sur la sécurité intérieure de l'Europe.

Ces deux éléments ont fait apparaître avec davantage d'acuité la nécessité de coordonner et de renforcer, de manière globale, les cadres de coopération de l'UE en matière de gestion des frontières, de migration et de sécurité ainsi que les outils d'information. La gestion des frontières, le contrôle de l'application de la loi et le contrôle des migrations sont intrinsèquement liés. Il est de notoriété publique que des citoyens de l'Union ont franchi les frontières extérieures pour se rendre dans des zones de conflit à des fins terroristes et représentent un danger à leur retour dans l'UE. Il apparaît que des terroristes ont emprunté des itinéraires de migration irrégulière pour pénétrer dans l'UE puis qu'ils se sont déplacés dans l'espace Schengen sans être repérés.

Le programme européen en matière de sécurité et l'agenda européen en matière de migration ont défini la voie à suivre pour la conception et la mise en œuvre de la stratégie de l'UE visant à relever les défis parallèles que constituent la gestion des migrations et la lutte contre le terrorisme et la criminalité organisée. La présente communication s'appuie sur les synergies entre ces deux textes et se veut un point de départ pour un débat sur la manière dont les systèmes d'information existants et futurs pourraient contribuer à améliorer tant la gestion des frontières extérieures que la sécurité intérieure de l'UE. Elle complète la proposition de décembre 2015 relative à la création d'un corps européen de garde-frontières et de garde-côtes et à l'amélioration de la prévention des crises et de l'intervention aux frontières extérieures.

Il existe un certain nombre de systèmes d'information à l'échelle de l'Union qui fournissent aux garde-frontières et aux policiers des informations utiles sur les personnes, mais l'architecture européenne de la gestion des données n'est pas parfaite. La présente communication esquisse certaines options possibles pour optimiser les avantages des systèmes d'information existants et pour concevoir, si nécessaire, de nouvelles actions complémentaires visant à combler les lacunes. Elle souligne également la nécessité d'améliorer à long terme l'interopérabilité des systèmes d'information, un objectif également mis en évidence par le Conseil européen et le Conseil[1], et présente des pistes pour le développement futur des systèmes d'information afin que les garde-frontières, autorités douanières, policiers et autorités judiciaires disposent des informations nécessaires.

[1] Conclusions du Conseil européen des 17 et 18 décembre 2015; déclaration commune des ministres européens de la justice et de l'intérieur et des représentants des institutions de l'UE sur les attentats terroristes perpétrés le 22 mars 2016 à Bruxelles (24 mars 2016); conclusions du Conseil de l'UE et des États membres, réunis au sein du Conseil, sur la lutte contre le terrorisme (20 novembre 2015).

Toute initiative future sera élaborée sur la base des principes de l'amélioration de la réglementation et fera l'objet d'une consultation publique et d'une analyse d'impact, y compris en ce qui concerne les droits fondamentaux et, en particulier, le droit à la protection des données à caractère personnel.

2. PROBLEMES A RESOUDRE

En raison de l'absence de frontières intérieures dans l'espace Schengen, il est indispensable d'avoir une gestion rigoureuse et fiable des mouvements de personnes aux frontières extérieures. Il s'agit d'une condition sine qua non pour garantir un niveau élevé de sécurité intérieure et la libre circulation des personnes au sein de cet espace. Dans le même temps, l'absence de frontières intérieures signifie que les autorités des États membres chargées de faire appliquer la loi ont aussi accès aux données pertinentes sur les personnes. On dénombre, à l'échelle de l'Union, plusieurs systèmes d'information et bases de données qui, conformément à leurs finalités respectives, fournissent aux garde-frontières, à la police et à d'autres autorités des informations pertinentes sur les personnes[2].

Cependant, certaines insuffisances des systèmes d'information empêchent le travail de ces autorités nationales. C'est la raison pour laquelle le programme européen en matière de sécurité a fait de l'amélioration de l'échange d'informations une priorité essentielle. Les principales insuffisances observées sont les suivantes: (a) fonctionnalités non optimales des systèmes d'information existants, (b) lacunes dans l'architecture de la gestion des données de l'UE, (c) mosaïque complexe de systèmes d'information régis de différentes façons et (d) architecture fragmentée de la gestion des données appliquée aux contrôles aux frontières et à la sécurité.

Les systèmes d'information utilisés actuellement dans l'UE pour la gestion des frontières et la sécurité intérieure couvrent un large éventail de fonctionnalités. Toutefois, celles-ci **présentent encore des insuffisances**. Lorsque l'on se penche sur les processus de contrôle aux frontières applicables à différentes catégories de voyageurs, il apparaît clairement que certains d'entre eux sont défaillants ou qu'il existe des failles entre les différents systèmes d'information utilisés pour les contrôles aux frontières. De même, le fonctionnement des outils utilisés à des fins répressives doit être optimisé. Ce constat appelle des mesures pour améliorer les systèmes d'information existants (voir partie 5).

Par ailleurs, il existe des **lacunes dans l'architecture de la gestion des données de l'UE**. Des problèmes persistent pour les contrôles aux frontières de certaines catégories de voyageurs, tels que les ressortissants de pays tiers en possession d'un visa de longue durée. On constate en outre un déficit d'informations avant l'arrivée à la frontière en ce qui concerne les ressortissants de pays tiers exemptés de l'obligation de visa. Il conviendrait, dès lors, de réfléchir à la nécessité ou non de combler ces lacunes en mettant sur pied des systèmes supplémentaires d'information si nécessaire (voir partie 6).

Les garde-frontières et les policiers se heurtent à une **mosaïque complexe de systèmes d'information régis de différentes façons** au niveau de l'UE. Cette complexité est source de difficultés pratiques en particulier pour déterminer quelles bases de données il convient d'interroger dans une situation concrète. Par ailleurs, les États membres ne sont

[2] Voir la partie 4 pour une vue d'ensemble des systèmes d'information utilisés dans les domaines des frontières et de la sécurité et l'annexe 2 pour un inventaire plus détaillé.

pas tous connectés à l'ensemble des systèmes existants[3]. On pourrait réduire la complexité actuelle de l'accès aux systèmes d'information au niveau de l'UE en créant, au niveau national, une interface de recherche unique qui respecte les différentes finalités d'accès (voir partie 7.1).

L'actuelle architecture européenne de la gestion des données appliquée aux contrôles aux frontières et à la sécurité se caractérise par sa **fragmentation**. Celle-ci est due aux différents contextes institutionnels, juridiques et stratégiques dans lesquels ces systèmes ont vu le jour. Les informations sont stockées séparément dans différents systèmes qui sont rarement interconnectés. Les bases de données présentent des incohérences et les pratiques divergent en ce qui concerne l'accès des autorités compétentes aux données. Il peut en résulter des «angles morts», notamment pour les autorités chargées de faire appliquer la loi, car il peut être très difficile de mettre en relation des données fragmentaires. Il est, dès lors, nécessaire et urgent d'œuvrer à des solutions intégrées pour une meilleure accessibilité des données à des fins de gestion des frontières et de sécurité, dans le plein respect des droits fondamentaux. Pour ce faire, il est nécessaire de lancer une procédure visant à garantir l'interopérabilité des systèmes d'information existants (voir partie 7).

3. DROITS FONDAMENTAUX

Le respect total des droits fondamentaux et des règles relatives à la protection des données est une condition sine qua non pour la recherche de solutions aux problèmes exposés ci-dessus.

Le respect des droits fondamentaux passe par des systèmes informatiques bien conçus et correctement utilisés. Les systèmes informatiques peuvent, en effet, aider les pouvoirs publics à protéger les droits fondamentaux des citoyens. Les techniques biométriques peuvent réduire le risque d'erreurs d'identité, de discrimination et de profilage racial. Elles peuvent également contribuer à mieux pallier les risques en matière de disparition ou de traite d'enfants, pour autant qu'elles s'accompagnent de garanties relatives aux droits fondamentaux et de mesures de protection. Elles peuvent réduire les risques d'interpellation et d'arrestation arbitraires. Elles peuvent également contribuer à renforcer la sécurité des citoyens résidant dans l'espace Schengen, étant donné qu'elles contribueront à la lutte contre le terrorisme et les formes graves de criminalité.

L'existence de systèmes d'information à grande échelle présente également des risques potentiels pour le droit au respect de la vie privée, qu'il convient d'anticiper et à l'égard desquels il importe de prendre des mesures adéquates. La collecte et l'utilisation de données à caractère personnel stockées dans ces systèmes ont une incidence sur les droits au respect de la vie privée et à la protection des données à caractère personnel, consacrés par la Charte des droits fondamentaux de l'Union européenne. Tous les systèmes doivent respecter les principes de protection des données et les exigences en matière de nécessité, de proportionnalité, de limitation des finalités et de qualité des données. Des garanties doivent être instituées pour protéger les droits des personnes concernées dans le domaine de la vie privée et des données à caractère personnel. Les données ne devraient être conservées que le temps nécessaire pour remplir la finalité pour laquelle elles ont été collectées. Il convient de prévoir des mécanismes garantissant une gestion adéquate des risques et une protection efficace des droits des personnes concernées.

[3] Sous réserve des dispositions particulières du protocole 22 en ce qui concerne le Danemark, des protocoles 21 et 36 en ce qui concerne le Royaume-Uni et l'Irlande et des différents actes d'adhésion.

En décembre 2015, les colégislateurs ont conclu un accord politique sur la réforme de la protection des données. Après leur adoption, le nouveau règlement général sur la protection des données et la directive relative à la protection des données destinées aux autorités policières et judiciaires pénales[4] entreront en application en 2018 et fourniront un cadre harmonisé pour le traitement des données à caractère personnel.

La limitation des finalités est un principe essentiel de la protection des données, inscrit dans la Charte des droits fondamentaux. En raison des contextes institutionnels, juridiques et stratégiques différents dans lesquels les systèmes d'information ont vu le jour dans l'UE, le principe de limitation des finalités a été mis en œuvre au moyen d'une structure compartimentée de la gestion de l'information[5]. C'est l'une des raisons de la fragmentation actuelle de l'architecture de la gestion des données de l'UE appliquée aux contrôles aux frontières et à la sécurité intérieure. Grâce à l'instauration du nouveau cadre général de protection des données à caractère personnel dans l'UE et aux progrès considérables accomplis dans les domaines technologique et de la sécurité informatique, le principe de limitation des finalités peut être plus facilement mis en œuvre en ce qui concerne l'accès aux données stockées et leur utilisation , dans le strict respect de la Charte des droits fondamentaux et de la jurisprudence récente de la Cour de justice de l'Union européenne. Les mesures telles que la compartimentation des données au sein d'un système et les règles d'accès et d'utilisation propres à chaque catégorie de données et d'utilisateurs devraient garantir la limitation nécessaire des finalités dans les solutions intégrées de gestion des données. Cela ouvre la voie à l'interopérabilité de systèmes d'information nécessairement assortis de règles strictes en matière d'accès et d'utilisation, sans répercussions sur l'actuel principe de limitation des finalités.

Les principes de «protection des données dès la conception» et de «protection des données par défaut» font désormais partie des dispositions de l'UE relatives à la protection des données. Lorsqu'elle élaborera de nouveaux instruments reposant sur l'utilisation des technologies de l'information, la Commission s'attachera à suivre cette approche. Pour ce faire, elle intégrera la protection des données à caractère personnel dans la base technologique des instruments proposés, en limitant le traitement des données au strict nécessaire compte tenu de la finalité précisée et en n'accordant l'accès aux données qu'aux entités ayant «besoin d'en connaître»[6].

Les exigences de la Charte des droits fondamentaux, en particulier en ce qui concerne les nouveaux instruments issus de la réforme de la protection des données, fourniront des indications utiles à la Commission pour combler les lacunes et les insuffisances actuelles de l'architecture de la gestion des données de l'UE appliquée aux contrôles aux frontières et à la sécurité. Ainsi, le développement plus poussé des systèmes d'information dans ces domaines se fera en conformité avec les normes les plus élevées de protection des données et ces systèmes respecteront les droits fondamentaux consacrés par la Charte des droits fondamentaux tout en y contribuant.

---

4 Voir http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

5 COM(2010) 385 final.

6 Pour une description complète du principe de «protection de la vie privée dès la conception», voir l'avis du Contrôleur européen de la protection des données du 18.3.2010 sur la promotion de la confiance dans la société de l'information grâce au renforcement de la protection des données et de la vie privée (Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy – disponible uniquement en anglais).

4. VUE D'ENSEMBLE DES SYSTEMES D'INFORMATION UTILISES POUR LA GESTION DES FRONTIERES ET LA SECURITE[7]

Les systèmes d'information utilisés actuellement dans l'UE pour la gestion des frontières et la sécurité intérieure ont chacun leurs propres objectifs, finalités, bases juridiques[8], groupes d'utilisateurs et contexte institutionnel. Considérés dans leur ensemble, ils constituent une combinaison complexe de bases de données pertinentes.

Les trois **principaux systèmes d'information centralisés** conçus par l'UE sont i) le système d'information Schengen (SIS), qui comporte toute une série de signalements concernant des personnes et des objets, ii) le système d'information sur les visas (VIS), qui contient des données sur les visas de court séjour, et iii) le système EURODAC, qui sert à stocker les données dactyloscopiques des demandeurs d'asile et des ressortissants de pays tiers ayant franchi irrégulièrement les frontières extérieures. Ces trois systèmes sont complémentaires et, à l'exception du SIS, concernent essentiellement les ressortissants de pays tiers. Ils aident également les autorités nationales à lutter contre la criminalité et le terrorisme[9]. C'est particulièrement vrai pour le SIS, qui est l'instrument d'échange d'informations le plus utilisé actuellement. L'échange d'informations dans le cadre de ces systèmes se fait grâce à une infrastructure de communication dédiée et sécurisée, appelée sTESTA[10].

Outre ces systèmes existants, la Commission propose de créer un quatrième système de gestion centralisé des frontières, le **système d'entrée/sortie** (Entry-Exist System - EES)[11], qui devrait être mis en service d'ici 2020, et qui concerne également les ressortissants de pays tiers.

---

7 Voir l'annexe 2 pour un inventaire des systèmes d'information utilisés actuellement pour la gestion des frontières et le contrôle de l'application de la loi.

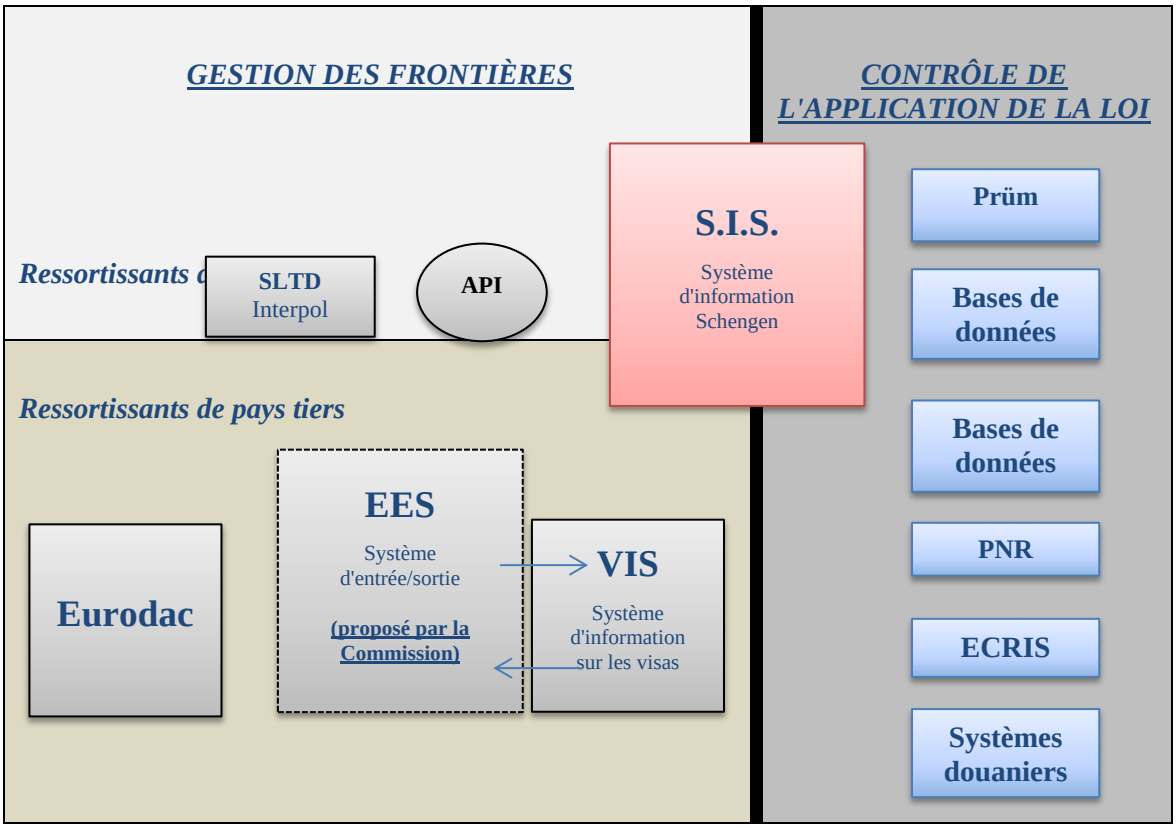
8 Sous réserve des dispositions particulières du protocole 22 en ce qui concerne le Danemark, et des protocoles 21 et 36 en ce qui concerne le Royaume-Uni et l'Irlande.

9 L'accès au VIS et à EURODAC à des fins répressives est assorti de certaines conditions, cette finalité étant un objectif secondaire de ces systèmes. En ce qui concerne le VIS, les États membres doivent désigner une autorité chargée de contrôler l'accès à des fins répressives et la police doit, le cas échéant, prouver que l'accès au système est nécessaire pour les besoins d'une enquête pénale. Pour ce qui est d'EURODAC, l'autorité d'enquête doit d'abord interroger le système AFIS national ainsi que les bases Prüm et VIS, avant de pouvoir avoir accès à EURODAC.

10 Sera bientôt remplacée par TESTA-NG.

11 COM(2016) 194 final.

Schéma n° 1 *Schéma des principaux systèmes d'information pour la gestion des frontières et le contrôle de l'application de la loi*



Parmi les autres instruments déjà utilisés pour la gestion des frontières, il convient de mentionner la base de données d'Interpol sur les documents de voyage perdus ou volés (SLTD) et le système d'informations préalables sur les passagers (API), qui sert à collecter des renseignements sur les passagers aériens préalablement à leur vol à destination de l'UE. Ces instruments sont utilisés tant pour les citoyens de l'Union que pour les ressortissants de pays tiers.

L'UE a créé des **outils décentralisés d'échange d'informations** destinés spécifiquement à des fins répressives, d'enquêtes pénales et de coopération judiciaire. Il s'agit i) du cadre institué à la suite du traité de Prüm pour l'échange d'ADN, d'empreintes digitales et de données relatives à l'immatriculation des véhicules (ci-après le «cadre Prüm») et ii) du système européen d'information sur les casiers judiciaires (ECRIS), qui permet d'échanger des informations provenant des casiers judiciaires nationaux. ECRIS permet l'échange d'informations, au moyen d'un réseau sécurisé, sur les condamnations antérieures prononcées par des juridictions pénales de l'Union européenne à l'encontre d'une personne déterminée. Les demandes sont fondées essentiellement sur des données d'identification alphanumériques, même si l'échange de données biométriques est également possible.

En tant que plateforme centrale de l'UE en matière d'informations sur la criminalité, **Europol** soutient l'échange d'informations entre autorités de police nationales. Le système d'information Europol (SIE) est une base de données centralisée qui permet aux États membres de stocker des données sur les formes graves de criminalité et le terrorisme et d'y effectuer des recherches. Les points de contact à Europol fournissent des fichiers de travail à des fins d'analyse qui contiennent des informations sur les opérations en cours dans les États membres. L'application de réseau d'échange sécurisé d'informations (SIENA) d'Europol permet aux États membres d'échanger des

informations de façon rapide, sûre et commode entre eux, avec Europol ou avec des tiers liés par un accord de coopération avec cette agence. Par ailleurs, SIENA est fortement axée sur l'interopérabilité avec les autres systèmes utilisés à Europol, par exemple l'échange direct de données avec les points de contact. L'application prévoit la possibilité d'alimenter les bases de données d'Europol en informations échangées entre États membres. Les États membres devraient, dès lors, faire de SIENA leur canal privilégié de partage d'informations en matière répressive dans l'UE.

Un autre système de traitement des données à caractère personnel sera mis en place dans l'ensemble des États membres: il s'agit du système de **dossiers passagers** (PNR)[12]. Les données PNR sont les informations fournies par chaque passager lors de la réservation et de l'enregistrement.

Enfin, les **autorités douanières** sont également un acteur incontournable de la coopération interagences aux frontières extérieures. Elles disposent de plusieurs systèmes[13] et bases de données contenant des données relatives aux mouvements de marchandises, à l'identification des opérateurs économiques et aux risques, qui peuvent être utilisées pour renforcer la sécurité intérieure. Ces systèmes fonctionnent, eux aussi, grâce à leur propre infrastructure contrôlée, restreinte et sécurisée (réseau commun de communications), dont la viabilité n'est plus à prouver. Il conviendrait d'explorer davantage les synergies et les convergences entre les systèmes d'information et leurs infrastructures correspondantes utilisés pour la gestion des frontières de l'UE et pour des opérations douanières.

5. AMELIORER LES SYSTEMES D'INFORMATION EXISTANTS

Les systèmes d'information qui existent dans l'UE pour la gestion des frontières et la sécurité intérieure couvrent un large éventail de fonctionnalités. Ils continuent toutefois à présenter des **lacunes** auxquelles il convient de remédier afin d'en optimiser les performances.

Système d'information Schengen (SIS)

Les vérifications aux frontières dans le cadre du **système d'information Schengen** (SIS) sont actuellement effectuées sur la base de consultations alphanumériques (c'est-à-dire avec un nom et une date de naissance). Les empreintes digitales ne peuvent être utilisées que pour vérifier et confirmer l'identité d'une personne qui a déjà été identifiée à partir de son nom. Cette faille de sécurité permet à des personnes faisant l'objet d'un signalement d'utiliser de faux documents pour échapper à une concordance dans le SIS.

Pour remédier à cette défaillance grave, une fonctionnalité de recherche dactyloscopique sera ajoutée au SIS sous la forme d'un **système automatisé d'identification des empreintes digitales (AFIS)**, conformément au cadre juridique existant[14]. Le système

---

[12] Voir la partie 6.2.

[13] Les systèmes d'information douaniers englobent tous les systèmes créés en vertu du code des douanes communautaires [règlement (CEE) n° 2913/92], du code des douanes de l'Union qui lui a succédé [règlement (UE) n° 952/2013] et de la décision relative à un environnement sans support papier pour la douane et le commerce [décision n° 70/2008/CE], ainsi que le système d'information douanier institué en vertu de la convention SID de 1995. Ils visent à contribuer à la lutte contre la criminalité douanière en facilitant la coopération entre les autorités douanières européennes.

[14] Article 22, point c), du 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), et article 22, point c), de la

AFIS devrait être opérationnel pour la mi-2017[15]. Lorsqu'il sera en place, ce système sera accessible à Europol et complétera par conséquent ses systèmes d'enquêtes pénales et de lutte contre le terrorisme, ainsi que les échanges d'empreintes digitales effectués au titre du cadre Prüm. La Commission et l'eu-LISA examineront la faisabilité de cet usage plus étendu du futur système AFIS.

Sur la base de l'évaluation en cours et d'une étude technique, la Commission explore actuellement la **possibilité d'ajouter des fonctionnalités au SIS** afin de présenter des propositions révisant la base juridique de ce système. Les aspects étudiés sont notamment:

- la création de signalements dans le SIS sur les migrants en situation irrégulière faisant l'objet d'une décision de retour,
- l'utilisation d'images faciales aux fins d'identification biométrique, en complément des empreintes digitales,
- la transmission automatisée d'informations en cas de réponse positive à l'issue d'une vérification,
- le stockage dans le système central du SIS des réponses positives à des signalements aux fins d'un contrôle discret ou d'un contrôle spécifique,
- la création d'une nouvelle catégorie de signalement dénommée «Wanted Unknown Person» (personne inconnue recherchée) pour laquelle il peut exister des données de police scientifique dans les bases de données nationales (par exemple une empreinte latente laissée sur la scène d'une infraction)[16].

La Commission continuera à soutenir par des financements de l'UE la mise en œuvre de projets permettant d'effectuer des recherches simultanées dans le SIS et les bases de données d'Interpol sur les documents de voyage perdus ou volés (SLTD) et sur les criminels, véhicules ou armes à feu recherchés (iARMS), qui complètent les systèmes d'information de l'UE[17].

Base de données d'Interpol sur les documents de voyage perdus ou volés (SLTD)

Il est essentiel, pour assurer une gestion efficace des frontières, que les documents de voyage présentés par tous les ressortissants de pays tiers et les citoyens de l'Union soient vérifiés par consultation de la **base de données SLTD**. Les autorités chargées de faire appliquer la loi devraient également interroger cette base de données pour des recherches à l'intérieur de l'espace Schengen. Après les attaques terroristes du 13 novembre 2015 à Paris, le Conseil a demandé, pour mars 2016, une connexion électronique avec les bases de données pertinentes d'Interpol à tous les points de passage des frontières extérieures et la vérification automatique des documents de voyage[18]. Tous les États membres sont

décision 533/2007/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 2015 du 7.8.2007, p. 63).

15 En mars 2016, la Commission a présenté un rapport au Parlement européen et au Conseil intitulé «La disponibilité et le degré de maturité de la technologie permettant d'identifier une personne sur la base des empreintes digitales contenues dans le système d'information Schengen de deuxième génération (SIS II)».

16 La création de ce nouveau signalement sera évaluée en recherchant une complémentarité et en évitant les redondances avec le cadre Prüm existant pour la recherche d'empreintes dans les différentes bases de données nationales des États membres de l'UE.

17 Les outils de recherche mis au point par Interpol, tels que les bases de données FIND (Fixed Interpol Networked Database) et MIND (Mobile Interpol Networked Database), visent à faciliter les recherches simultanées dans les systèmes d'Interpol et dans le SIS.

18 Conclusions du Conseil de l'UE et des États membres, réunis au sein du Conseil, sur la lutte contre le terrorisme, 20 novembre 2015.

tenus de créer les connexions électroniques correspondantes et de mettre en place des systèmes permettant la mise à jour automatique des données sur les documents de voyage perdus ou volés dans la base SLTD.

Informations préalables sur les passagers (API)

Conformément aux bonnes pratiques existantes, les États membres devraient également accroître la valeur ajoutée des données relatives aux **informations préalables sur les passagers** (API) en instaurant une vérification croisée automatique de ces données par rapport au SIS et à la base SLTD d'Interpol. La Commission évaluera la nécessité de réviser la base juridique du traitement des données API pour assurer une mise en œuvre plus étendue et obliger en outre les États membres à demander et à utiliser lesdites données pour la totalité des vols entrants et sortants. Cette démarche revêt une importance particulière dans le cadre de l'application de la future directive sur les données PNR (données des dossiers passagers), car l'utilisation combinée des données PNR et API renforce l'efficacité de l'utilisation des données PNR dans la lutte contre le terrorisme et les formes graves de criminalité[19].

Système d'information sur les visas (VIS)

La Commission procède également à une évaluation globale du **système d'information sur les visas** (VIS), qui devrait s'achever en 2016. L'évaluation porte notamment sur la manière dont le VIS est utilisé pour les vérifications aux frontières extérieures et à l'intérieur du territoire des États membres, et examine en quoi il contribue à la lutte contre l'usurpation d'identité et la fraude aux visas. Sur cette base, la Commission étudiera ensuite les possibilités de renforcer les fonctionnalités du VIS, notamment:

- en améliorant la qualité des images faciales pour permettre la mise en correspondance biométrique,
- en utilisant les données biométriques des demandeurs de visa pour effectuer des recherches dans le futur système automatisé d'identification des empreintes digitales qui sera mis en place pour le SIS,
- en abaissant l'âge limite fixé pour le relevé des empreintes digitales des enfants âgés de 6 à 12 ans, tout en instaurant des garanties solides en matière de droits fondamentaux et des mesures de protection[20],
- en facilitant la vérification dans la base de données SLTD d'Interpol lors des procédures de demande de visa.

En ce qui concerne les possibilités prévues par le cadre juridique en vigueur pour accéder aux données du VIS **à des fins répressives**, les États membres les appliquent de manière inégale. Ils ont signalé dans ce contexte des problèmes pratiques dans les procédures d'accès au VIS utilisées par les autorités chargées de faire appliquer la loi. De la même manière, la mise en œuvre de l'accès à EURODAC à des fins répressives est encore très limitée. La Commission examinera s'il est nécessaire de revoir le cadre juridique de l'accès au VIS et à EURODAC à des fins répressives.

EURODAC

Comme elle l'indique dans la communication intitulée «Vers une réforme du régime d'asile européen commun et une amélioration des voies d'entrée légale en Europe»[21], la Commission proposera de réformer **EURODAC** de manière à étendre ses fonctionnalités

[19] Voir partie 6.2, sur la proposition de directive relative aux données PNR.

[20] Selon les possibilités techniques exposées dans l'étude du CCR intitulée «Fingerprint Recognition for children», EUR 26193 EN; ISBN 978-92-79-33390-3Children, 2013.

[21] COM(2016) 197 final.

par rapport aux migrations irrégulières et aux retours. Cela permettra de combler une lacune existante quant à la possibilité de suivre les mouvements secondaires des migrants en question d'un État membre à l'autre. De plus, la proposition visera à renforcer l'efficacité des procédures de retour et de réadmission, en prévoyant des moyens d'identifier les migrants en situation irrégulière et de leur délivrer de nouveaux documents d'identité aux fins du retour. Dans ce contexte, la proposition couvrira également l'échange avec les pays tiers d'informations contenues dans EURODAC, en n'oubliant pas les garanties nécessaires en matière de protection des données.

Europol

L'UE a accordé à **Europol** l'accès aux principales bases de données centrales, mais l'agence n'a pas encore utilisé pleinement cette possibilité. Europol a le droit d'accéder aux données saisies dans le SIS et de les consulter directement en ce qui concerne les arrestations, les contrôles discrets ou les contrôles spécifiques et les objets recherchés aux fins de saisie. Jusqu'à présent, Europol n'a effectué qu'un nombre de recherches relativement limité dans le SIS. L'accès au VIS pour consultation est juridiquement autorisé pour Europol depuis septembre 2013. Depuis juillet 2015, la base juridique sur laquelle est fondé EURODAC permet à Europol d'y accéder. L'agence devrait accélérer les travaux en cours afin d'établir des connexions avec le VIS et EURODAC. Plus généralement, la Commission évaluera la nécessité d'autoriser ou non les autres agences de l'UE du domaine des affaires intérieures à avoir également accès aux systèmes d'information, notamment le futur corps européen de garde-frontières et de garde-côtes.

Cadre Prüm

À l'heure actuelle, le potentiel du **cadre Prüm** s'épuise, car les États membres n'ont pas tous mis en œuvre leurs obligations juridiques concernant l'intégration du réseau dans leurs propres systèmes. Les États membres ont reçu, à cette fin, un appui financier et technique important et devraient à présent appliquer intégralement le cadre Prüm. Faisant usage des prérogatives qui lui sont accordées pour veiller à l'exécution complète des obligations juridiques des États membres, la Commission a engagé un dialogue structuré (procédure EU Pilot) avec les États membres concernés, en janvier 2016. Si les réponses apportées par les États membres devaient ne pas être satisfaisantes, la Commission n'hésitera pas à lancer des procédures d'infraction.

Système européen d'information sur les casiers judiciaires (ECRIS)

Le système européen d'information sur les casiers judiciaires **ECRIS** permet l'échange d'informations sur les condamnations pénales prononcées à l'encontre de ressortissants de pays tiers et de personnes apatrides, mais il n'existe aucune procédure permettant de mener efficacement cette démarche. En janvier 2016, la Commission a adopté une proposition législative pour combler cette lacune[22]. Dans ce contexte, elle a proposé d'offrir aux autorités nationales la possibilité de rechercher des ressortissants de pays tiers sur la base des empreintes digitales, pour que l'identification de ces derniers soit plus sûre. Cet instrument législatif devrait être adopté par le Parlement européen et le Conseil en 2016.

Questions horizontales

L'une des préoccupations générales relatives aux systèmes d'information porte sur le **niveau de mise en œuvre** par les États membres. L'application inégale du cadre Prüm et les connexions électroniques manquantes vers la base de données SLTD sont des

[22] COM(2016) 7 final du 19.1.2016.

exemples frappants à cet égard. Pour accroître le niveau de mise en œuvre relatif aux systèmes d'information, la Commission assurera un suivi étroit des réalisations des États membres[23]. Ce suivi lui permettra d'examiner non seulement si les États membres satisfont à leurs obligations juridiques dans le domaine des systèmes d'information, mais également la manière dont ils utilisent les instruments existants et s'ils appliquent les meilleures pratiques. La Commission s'appuiera sur diverses sources pour contrôler et faire progresser le niveau de mise en œuvre, notamment sur les notifications émises par les États membres et les inspections effectuées au titre du mécanisme d'évaluation et de contrôle Schengen.

Une autre préoccupation générale relative aux systèmes d'information concerne la **qualité des données saisies**. Si les États membres ne respectent pas les exigences de qualité minimales, la fiabilité et la valeur des données stockées s'en trouvent très limitées, et le risque de résultat erroné et de non-concordance diminue la valeur intrinsèque de ces systèmes. Afin d'améliorer la qualité des données saisies, l'agence eu-LISA mettra en place un **mécanisme central de suivi de la qualité des données**, pour l'ensemble des systèmes relevant de sa compétence.

La plupart des systèmes d'information en matière de contrôle aux frontières et de sécurité traitent des données d'identification provenant de documents de voyage et d'identité. Pour renforcer les frontières et la sécurité, il faut non seulement disposer de systèmes performants mais également authentifier de manière aisée et sûre les documents de voyage et d'identité. Pour ce faire, la Commission présentera des mesures visant à renforcer la **sécurité des documents** électroniques et la gestion des documents d'identité, ainsi que la lutte contre la fraude documentaire. Les niveaux interopérables d'identification sécurisée que l'on peut obtenir avec le règlement eIDAS[24] pourraient fournir un moyen d'y parvenir.

Actions visant à améliorer les systèmes d'information existants

Système d'information Schengen (SIS)

- La Commission et l'eu-LISA doivent mettre au point et en pratique une fonctionnalité AFIS (système automatisé d'identification des empreintes digitales) dans le SIS pour la mi-2017.
- La Commission doit présenter des propositions pour la fin 2016 en vue de réviser la base juridique du SIS pour continuer à développer sa fonctionnalité.
- Les États membres doivent optimiser l'utilisation du SIS, à la fois en y saisissant toutes les informations pertinentes et en consultant le système autant que nécessaire.

Base de données d'Interpol sur les documents de voyage perdus ou volés (SLTD)

- Les États membres doivent établir des connexions électroniques avec les outils d'Interpol à l'ensemble des points de passage de leurs frontières extérieures.
- Les États membres doivent respecter leur obligation de saisir et de consulter les données relatives aux documents de voyage perdus ou volés simultanément dans les bases de données SIS et SLTD.

[23] Sous réserve des dispositions particulières du protocole 22 en ce qui concerne le Danemark, et des protocoles 21 et 36 en ce qui concerne le Royaume-Uni et l'Irlande.

[24] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Informations préalables sur les passagers (API)

- Les États membres doivent automatiser l'utilisation des données API pour procéder aux vérifications par consultation du SIS et de la base de données d'Interpol relative aux documents de voyage perdus ou volés (SLTD), conformément aux meilleures pratiques existantes.
- La Commission doit évaluer la nécessité de réviser la base juridique du traitement des données API.

Système d'information sur les visas (VIS)

- La Commission doit envisager de nouvelles améliorations du VIS avant la fin 2016.

EURODAC

- La Commission doit présenter une proposition de révision de la base juridique d'EURODAC afin de continuer à développer ses fonctionnalités par rapport aux migrations irrégulières et aux retours.

Europol

- Europol doit faire pleinement usage de ses droits d'accès existants au SIS, au VIS et à EURODAC aux fins de consultation.
- La Commission et Europol doivent rechercher et promouvoir des synergies entre le système d'information d'Europol (SIE) et d'autres systèmes, dont le SIS.
- La Commission et l'eu-LISA doivent évaluer si la fonctionnalité AFIS (système automatisé d'identification des empreintes digitales) qui doit être développée pour le SIS peut compléter les systèmes d'Europol à des fins d'enquêtes pénales et de lutte contre le terrorisme.

Cadre Prüm

- Les États membres doivent appliquer et utiliser pleinement le cadre Prüm.
- Si nécessaire, la Commission lancera des procédures d'infraction contre les États membres qui ne se seront pas connectés au cadre Prüm.
- La Commission et l'eu-LISA doivent évaluer si la fonctionnalité AFIS (système automatisé d'identification des empreintes digitales) qui doit être développée pour le SIS peut compléter les échanges de données dactyloscopiques effectués au titre du cadre Prüm.

Système européen d'information sur les casiers judiciaires (ECRIS)

- Le Parlement européen et le Conseil devraient adopter en 2016 la proposition législative permettant aux autorités nationales de rechercher des ressortissants de pays tiers dans l'ECRIS à partir des empreintes digitales.

Questions horizontales

- La Commission doit **contrôler et faire progresser le niveau de mise en œuvre** dans le domaine des systèmes d'information.
- L'agence eu-LISA doit mettre en place un **mécanisme central de suivi de la qualité des données**, pour l'ensemble des systèmes relevant de sa compétence.
- La Commission doit présenter des mesures visant à renforcer la **sécurité des documents électroniques et la gestion des documents d'identité**, ainsi que la lutte contre la fraude documentaire.

- La Commission doit rechercher des synergies et des convergences entre les systèmes d'information et leurs infrastructures correspondantes pour la gestion des frontières de l'UE et pour les **opérations douanières**.

6. ÉLABORER DES SYSTEMES D'INFORMATION SUPPLEMENTAIRES ET COMBLER LES LACUNES EXISTANTES

Si les systèmes d'information existants couvrent un très large éventail de données, conformément à ce qui est prévu dans le cadre de la gestion des frontières et du contrôle de l'application de la loi, d'importantes lacunes sont néanmoins à signaler. Certaines de ces lacunes ont été comblées par la Commission à l'aide de propositions législatives, en l'occurrence celle sur le système d'entrée/sortie et celle sur le système de données des dossiers passagers (PNR) de l'UE. Pour ce qui est des autres lacunes recensées, il convient d'examiner attentivement si des outils supplémentaires de l'UE sont nécessaires.

1. Système d'entrée/sortie

Parallèlement à la présente communication, la Commission a présenté des propositions législatives révisées en vue de la création d'un système d'entrée/sortie (EES). Une fois ce système adopté par les colégislateurs, il appartiendra à l'eu-LISA de l'élaborer et de le mettre en œuvre, en coopération avec les États membres faisant partie de l'espace Schengen.

L'EES enregistrera les franchissements de frontière (entrées et sorties) de tous les ressortissants de pays tiers qui se rendent dans l'espace Schengen pour un court séjour (90 jours maximum sur une période de 180 jours), qu'il s'agisse de voyageurs soumis à l'obligation de visa ou qui en sont exemptés, ou pour des séjours au titre du nouveau visa d'itinérance (jusqu'à un an). Les objectifs de l'EES sont a) d'améliorer la gestion des frontières extérieures, b) de réduire la migration irrégulière en s'attaquant au phénomène du dépassement de la durée de séjour autorisée et c) de contribuer à la lutte contre le terrorisme et les formes graves de criminalité en assurant, ce faisant, un niveau élevé de sécurité intérieure.

L'EES enregistrera l'identité des ressortissants de pays tiers (données alphanumériques, quatre empreintes digitales et image faciale), ainsi que les données figurant dans leurs documents de voyage, et établira un lien entre ces informations et les fiches électroniques d'entrée et de sortie. Il sera mis un terme à la pratique actuelle de l'apposition de cachets sur les documents de voyage. L'EES permettra de gérer efficacement les courts séjours autorisés, de renforcer l'automatisation aux points de passage frontaliers et d'améliorer la détection de la fraude documentaire et de l'usurpation d'identité. L'enregistrement centralisé permettra de repérer les personnes qui dépassent la durée de séjour autorisée et d'identifier les personnes sans papiers dans l'espace Schengen. L'EES, tel qu'il est proposé, comble dès lors une lacune de taille dans le paysage des systèmes d'information existants.

2. Données des dossiers passagers

Les données PNR se composent de confirmations de réservation comprenant des coordonnées, d'informations complètes relatives aux voyages et aux réservations, de remarques spéciales, d'informations relatives au siège et aux bagages et d'indications sur les moyens de paiement. Les données PNR sont à la fois utiles et nécessaires pour identifier les voyageurs présentant un risque élevé dans le contexte de la lutte contre le terrorisme, du trafic de stupéfiants, de la traite d'êtres humains, de l'exploitation sexuelle des enfants et d'autres formes graves de criminalité. La directive PNR proposée permettra

d'assurer une meilleure coopération entre les systèmes nationaux et de réduire les écarts en matière de sécurité entre les États membres. En cela, elle comble une importante lacune sur le plan de la disponibilité des données nécessaires à la lutte contre le terrorisme et les formes graves de criminalité. **La directive PNR devrait être adoptée, transposée et mise en œuvre d'urgence**.

La future directive veillera à ce que les États membres créent des unités d'informations passagers (UIP), qui recevront les données PNR communiquées par les transporteurs. La directive bénéficiera d'un certain degré de normalisation des solutions et procédures techniques nationales, sans imposer pour autant la création d'un système central ni d'une base de données centrale. L'échange de données PNR entre UIP s'en trouvera facilité, comme le prévoit la directive proposée. À cette fin, la Commission aidera les États membres à analyser différents scénarios d'interconnexion entre UIP, de manière à proposer des solutions et des procédures normalisées. Une fois la directive adoptée, la Commission accélérera les travaux sur les protocoles communs et les formats de données reconnus pour les transferts des données PNR par les transporteurs aériens vers les UIP. La Commission préparera un projet d'acte d'exécution dans les trois mois suivant l'adoption de la directive.

3. Manque d'informations préalablement à l'arrivée de ressortissants de pays tiers exemptés de l'obligation de visa

Si l'identité et les coordonnées des titulaires de visas, ainsi que les informations générales les concernant sont enregistrées dans le VIS, les seules informations disponibles sur les personnes exemptées de l'obligation de visa figurent dans leur document de voyage. Pour les personnes voyageant par voie aérienne ou maritime, ce manque d'informations peut être comblé avant leur arrivée par les données API. En vertu de la directive PNR proposée, leurs données PNR seront également collectées si elles arrivent dans l'UE par voie aérienne. Pour les personnes entrant dans l'UE en franchissant les frontières terrestres, aucune information n'est disponible avant leur arrivée aux frontières extérieures de l'Union.

Alors que les autorités chargées du contrôle de l'application de la loi peuvent obtenir des informations sur les titulaires de visas à partir du VIS, si cela est nécessaire pour lutter contre les formes graves de criminalité et le terrorisme, aucune donnée comparable n'est disponible en ce qui concerne les personnes exemptées de l'obligation de visa. Ce manque d'informations est particulièrement problématique pour la gestion des frontières terrestres de l'UE, alors qu'un grand nombre de voyageurs exemptés de l'obligation de visa arrivent en voiture, en bus ou en train. Plusieurs pays voisins de l'UE sont déjà dispensés de l'obligation de visa et des dialogues sur la libéralisation du régime des visas entre l'UE et d'autres pays voisins ont été engagés. Ces démarches pourraient conduire à une forte augmentation du nombre de voyageurs exemptés de l'obligation de visa dans un proche avenir.

La Commission examinera l'utilité, la faisabilité et la proportionnalité d'un nouvel outil de l'UE pour régler ce problème. Un **système de l'UE d'information et d'autorisation concernant les voyages** (ETIAS) pourrait être envisagé. Les voyageurs exemptés de l'obligation de visa y entreraient des informations pertinentes concernant le voyage qu'ils prévoient d'effectuer. Le traitement automatique de ces informations pourrait aider les garde-frontières dans leur évaluation des visiteurs ressortissants de pays tiers arrivant pour un court séjour. Certains pays, tels que les États-Unis, le Canada et l'Australie, ont déjà mis en place des systèmes similaires, y compris pour les citoyens de l'UE.

Les systèmes d'autorisation de voyage sont basés sur des inscriptions électroniques par lesquelles le candidat au voyage fournit des informations concernant son identité, ses coordonnées, l'objet de son voyage, son itinéraire, etc. avant le départ. Une fois l'autorisation obtenue, les procédures de vérification aux frontières à l'arrivée gagnent en rapidité et en fluidité. Au-delà des avantages qu'il procure en matière de sécurité et de gestion des frontières et de son intérêt potentiel dans le contexte de la réciprocité en matière de visas, un système tel que le système ETIAS servirait également d'outil permettant de faciliter les voyages.

4. Système d'index européen des registres de la police (EPRIS)

Ainsi qu'il est indiqué dans le programme européen en matière de sécurité, la disponibilité en temps réel des données policières existant dans l'ensemble des États membres sera l'objet de travaux futurs en matière d'échange d'informations. La Commission appréciera l'utilité, la faisabilité technique et la proportionnalité d'un système d'index européen des registres de la police (EPRIS) destiné à faciliter l'accès transfrontière aux informations conservées dans les bases de données des services répressifs nationaux. Dans ce contexte, la Commission soutient, à l'aide de financements de l'UE, la mise en œuvre, par un groupe de cinq États membres, d'un projet pilote visant à instaurer un mécanisme de recherche transfrontière automatisée dans les index nationaux sur la base d'un système de concordance/non-concordance[25]. La Commission tiendra compte des résultats de ce projet dans son évaluation.

<u>Actions visant à élaborer des systèmes d'information supplémentaires et à combler les lacunes en matière d'information</u>

Système d'entrée/sortie (EES)

- Le Parlement européen et le Conseil devraient traiter les propositions législatives concernant l'EES comme une priorité absolue, de manière à ce que les propositions soient adoptées d'ici fin 2016.

Données des dossiers passagers (PNR)

- Le Parlement européen et le Conseil devraient adopter la directive PNR en avril 2016.
- Les États membres transposeront et mettront en œuvre d'urgence la directive PNR dès son adoption.
- La Commission soutiendra l'échange de données entre unités d'informations passagers au moyen de solutions et de procédures normalisées.
- La Commission préparera un projet de décision d'exécution sur les protocoles communs et les formats de données reconnus pour les transferts de données PNR par les transporteurs aériens vers les UIP dans les trois mois suivant l'adoption de la directive PNR.

[25] Le projet pilote concernant un processus d'échange automatisé de données (ADEP) vise à créer un système technique permettant, à l'aide d'un index, de savoir si un individu fait l'objet d'une inscription dans les registres de la police ou d'une enquête de police judiciaire en cours dans un ou plusieurs autres États membres. La réponse automatisée à une recherche dans l'index indiquerait seulement si des données sont disponibles (concordance) ou pas (non-concordance). Des données à caractère personnel supplémentaires devraient être demandées dans un deuxième temps, en cas de concordance, via les canaux habituels de coopération policière.

Manque d'informations préalablement à l'arrivée de ressortissants de pays tiers exemptés de l'obligation de visa

- La Commission évaluera, en 2016, l'utilité, la faisabilité technique et la proportionnalité de la création d'un nouvel outil, tel qu'un système de l'UE d'information et d'autorisation concernant les voyages.

Système d'index européen des registres de la police (EPRIS)

- La Commission évaluera, en 2016, l'utilité, la faisabilité technique et la proportionnalité de la mise en place d'un système d'index européen des registres de la police.

7. VERS L'INTEROPERABILITE DES SYSTEMES D'INFORMATION

L'interopérabilité est la capacité des systèmes d'information à échanger des données et à permettre le partage d'informations. On distingue **quatre dimensions en matière d'interopérabilité**, chacune d'elles posant des problèmes juridiques[26], techniques et opérationnels, y compris en matière de protection des données:

- une interface de recherche unique permettant d'interroger simultanément plusieurs systèmes d'information et de produire des résultats combinés sur un seul écran;
- l'interconnexion des systèmes d'information, qui permet aux données enregistrées dans un système d'être automatiquement consultées par un autre système;
- la mise en place d'un service partagé de mise en correspondance de données biométriques à l'appui de divers systèmes d'information;
- un répertoire commun de données pour différents systèmes d'information (module central).

Afin d'engager un processus conduisant à l'interopérabilité des systèmes d'information au niveau de l'UE, la Commission constituera, à haut niveau, **un groupe d'experts sur les systèmes d'information et l'interopérabilité** avec les agences de l'UE, des experts nationaux et les parties prenantes institutionnelles concernées. Ce groupe d'experts aura pour mission de se pencher sur les aspects juridiques, techniques et opérationnels des différentes options permettant de parvenir à l'interopérabilité des systèmes d'information, en examinant notamment l'utilité, la faisabilité technique et la proportionnalité des options disponibles et leurs conséquences sur le plan de la protection des données. Il devrait s'employer à combler les lacunes existantes et à pallier les insuffisances actuelles en matière d'information résultant de la complexité et de la fragmentation des systèmes d'information au niveau européen. Le groupe d'experts suivra une approche large et globale en matière de gestion des frontières et de contrôle de l'application de la loi, en tenant compte également du rôle joué par les autorités douanières à cet égard, de leurs responsabilités et des systèmes qu'elles utilisent. Les méthodes de travail employées par le groupe auront pour but de créer des synergies entre l'ensemble des expériences en la matière, qui ont trop souvent été cloisonnées par le passé.

L'objectif de ce processus est de fournir une vision stratégique globale de l'architecture européenne de gestion des données en matière de contrôle aux frontières et de sécurité, tout en apportant des solutions pour sa mise en œuvre.

Ce processus de consultation doit **avoir les objectifs suivants**:

[26] Sous réserve des dispositions particulières du protocole 22 en ce qui concerne le Danemark, et des protocoles 21 et 36 en ce qui concerne le Royaume-Uni et l'Irlande.

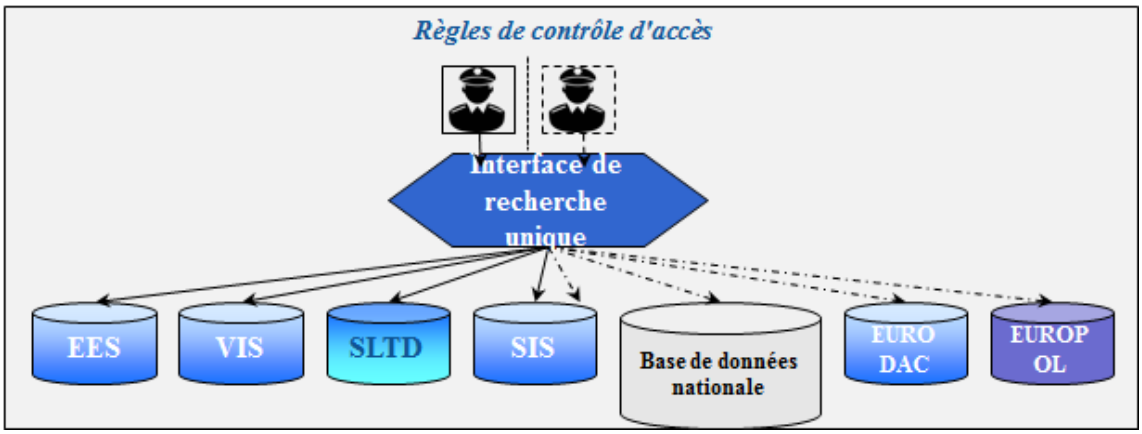
- Veiller à la complémentarité des systèmes d'information. Faire en sorte d'éviter les doublons et de supprimer les chevauchements existants. Combler les lacunes comme il se doit.
- Adopter une approche modulaire tirant le meilleur parti des progrès technologiques et s'appuyant sur les principes de la protection de la vie privée dès la conception.
- Assurer le respect total des droits fondamentaux des citoyens de l'Union et des ressortissants de pays tiers dès le départ, conformément à la Charte des droits fondamentaux.
- Lorsque cela s'avère nécessaire et faisable, veiller à l'interconnexion et à l'interopérabilité des systèmes d'information. Faciliter les recherches simultanées dans les différents systèmes, afin que les garde-frontières ou les agents de police puissent disposer de toutes les informations pertinentes où et quand ils en ont besoin pour leurs missions respectives, sans pour autant modifier les droits d'accès actuels.

1. Interface de recherche unique

La première dimension de l'interopérabilité est la **capacité**, offerte aux garde-frontières ou aux agents de police, **d'interroger simultanément plusieurs systèmes d'information et de produire des résultats combinés sur un seul écran,** en respectant pleinement leurs droits d'accès, eu égard à leurs objectifs respectifs. Cela nécessite des plateformes dotées d'une interface de recherche unique, qui sont capables de consulter simultanément divers systèmes d'information dans le cadre d'une seule interrogation. Ainsi, en lisant la puce d'un document de voyage ou en utilisant des données biométriques, cette plateforme pourrait interroger en même temps plusieurs bases de données différentes. La recherche unique concerne toutes les autorités ayant besoin d'accéder à des données et de les utiliser (en l'occurrence, les garde-frontières, les autorités chargées du contrôle de l'application de la loi et les services chargés de l'asile), en tenant compte de la limitation des finalités et des règles strictes en matière de contrôle des accès. Elle peut également être utilisée à partir d'un équipement mobile. La création d'une interface de recherche unique réduit la complexité des systèmes d'information au niveau européen, car cela permet aux garde-frontières et aux agents de police d'interroger simultanément plusieurs systèmes d'information au moyen d'une seule procédure, et en tenant compte de leurs droits d'accès spécifiques.

Plusieurs États membres ont déjà installé des plateformes similaires dotées d'une interface de recherche unique. En se fondant sur les bonnes pratiques existantes, la Commission et l'eu-LISA s'emploieront à trouver une solution d'interface de recherche unique normalisée. Les États-membres devraient utiliser les fonds de l'UE dans le cadre de leur programme national au titre du Fonds pour la sécurité intérieure pour financer l'installation de cette fonctionnalité. La Commission surveillera attentivement la manière dont les États membres se serviront de cette fonctionnalité au niveau national.

***Schéma n° 2** Interface de recherche unique*



Il est plus facile d'effectuer des recherches dans des systèmes centralisés ou nationaux multiples (comme dans le schéma ci-dessus) que dans des systèmes décentralisés. La Commission et l'eu-LISA examineront la possibilité d'utiliser également une interface de recherche unique pour effectuer simultanément, dans le cadre d'un guichet unique, des recherches sur des systèmes décentralisés, tels que Prüm et l'ECRIS. La Commission et l'eu-LISA effectueront cette analyse en concertation avec le groupe d'experts sur les systèmes d'information et l'interopérabilité, sans modifier les droits d'accès actuels.

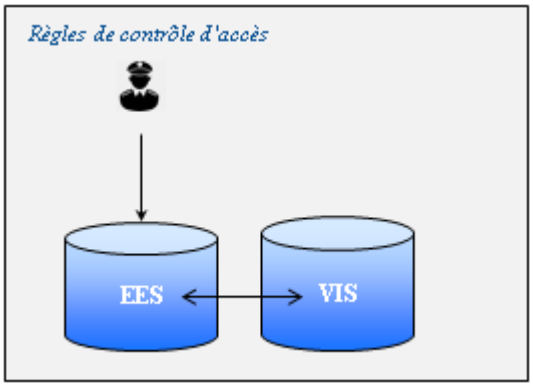
2. Interconnexion des systèmes d'information

Une deuxième dimension de l'interopérabilité est l'interconnexion des systèmes d'information. Cela signifie que différents systèmes ou bases de données sont techniquement capables de communiquer les uns avec les autres. **Il serait possible de consulter automatiquement des données enregistrées dans un système par un autre système à un niveau centralisé.** Il faut pour ce faire que les systèmes soient techniquement compatibles et que les éléments d'information stockés dans ces systèmes (empreintes digitales, par exemple) soient interopérables. L'interconnexion peut réduire la quantité de données circulant sur les réseaux de communication et transitant par des systèmes nationaux.

L'interconnexion nécessite des garanties appropriées en matière de protection des données et des règles strictes en matière de contrôle des accès. L'accord politique sur la réforme de la protection des données auquel sont parvenus les colégislateurs en décembre 2015 mettra en place dans l'ensemble de l'UE un cadre moderne de protection des données qui apportera les garanties en question. Il importe que les colégislateurs adoptent sans délai le règlement général sur la protection des données et la directive relative à la protection des données.

Le concept de l'interconnexion est intégré dans le futur système EES. Ce dernier sera capable de communiquer directement avec le VIS au niveau central et vice versa. Il s'agit là d'une mesure importante pour la résolution du problème actuel de la fragmentation de l'architecture européenne de gestion des données en matière de contrôle aux frontières et de sécurité, ainsi que des problèmes en découlant. Le contrôle croisé automatique des données dispensera les États membres d'interroger le VIS lors des vérifications aux frontières, réduira les besoins de maintenance et améliorera la performance du système.

Schéma n° 3 *Interconnexion des systèmes: l'exemple de l'EES/VIS*



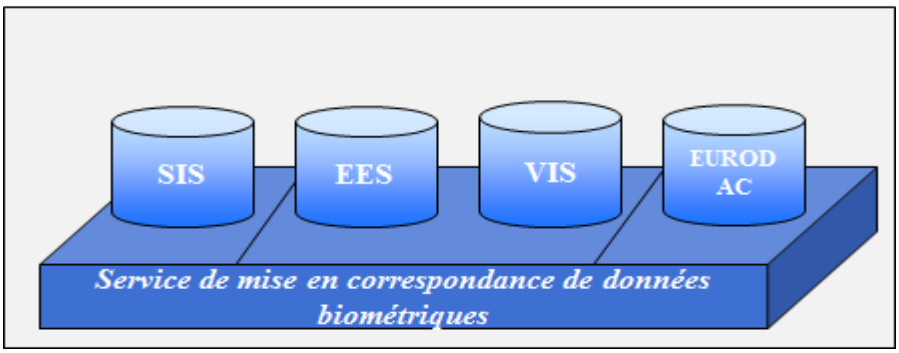
Dans un deuxième temps, la Commission et l'eu-LISA examineront si l'interconnexion au niveau central entre le futur EES et le VIS peut être étendue au SIS et si une interconnexion peut être établie entre EURODAC et le SIS. La Commission et l'eu-LISA effectueront cette analyse en concertation avec le groupe d'experts sur les systèmes d'information et l'interopérabilité.

3. Service partagé de mise en correspondance de données biométriques

Une troisième dimension de l'interopérabilité a trait aux identifiants biométriques. Par exemple, lorsque les empreintes digitales sont relevées au consulat d'un État membre doté d'un équipement spécifique, il est essentiel que ces empreintes puissent être mises en correspondance au moyen du VIS au poste frontière d'un autre État membre utilisant un équipement d'un autre type. La même règle s'applique aux recherches d'empreintes digitales dans d'autres systèmes: les échantillons biométriques doivent satisfaire à des critères minimums de qualité et de format pour assurer sans difficulté ce type d'interopérabilité.

Au niveau du système, l'interopérabilité des identifiants biométriques permet d'utiliser un service partagé de mise en correspondance de données biométriques pour plusieurs systèmes d'information, en respectant les règles de protection des données à caractère personnel, grâce à une compartimentation des données, et en instituant des règles distinctes en matière de contrôle d'accès pour chaque catégorie de données[27]. De tels services partagés procurent d'importants avantages sur les plans financier, opérationnel et de la maintenance.

Schéma n° 4 *Service partagé de mise en correspondance de données biométriques*



[27] Ce qui est comparable au partage d'un serveur de fichiers physique entre une multitude d'utilisateurs, chacun ayant des droits d'accès spécifiques à certains dossiers uniquement.

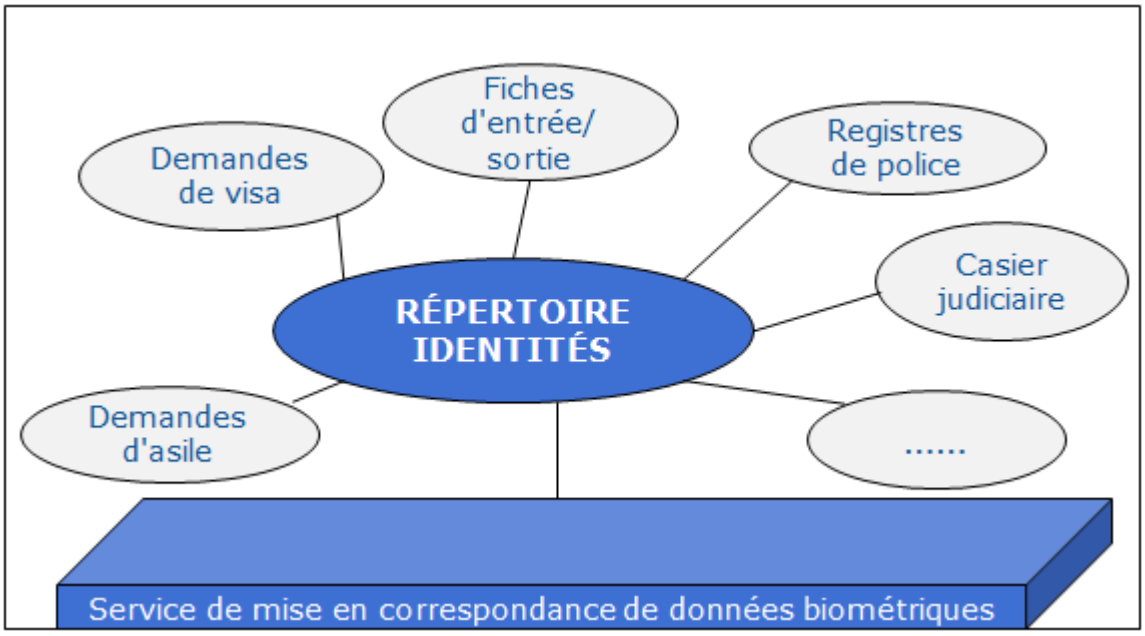
La Commission et l'eu-LISA examineront s'il est utile et techniquement réalisable de créer un service partagé de mise en correspondance de données biométriques pour tous les systèmes d'information pertinents. La Commission et l'eu-LISA effectueront cette analyse en concertation avec le groupe d'experts sur les systèmes d'information et l'interopérabilité.

4. Répertoire commun de données

L'approche la plus ambitieuse en matière d'interopérabilité à long terme consisterait à constituer un **répertoire commun de données au niveau de l'UE pour différents systèmes d'information**. Ce répertoire se présenterait sous la forme d'un module central contenant les données de base (données alphanumériques et biométriques), tandis que les autres éléments d'information et les caractéristiques propres aux différents systèmes d'information (données sur les visas, par exemple) seraient stockés dans des modules spécifiques. Le module central et les modules spécifiques seraient connectés les uns aux autres en vue de lier les ensembles de données respectifs. Il en résulterait une **gestion de l'identité modulaire et intégrée au service des frontières et de la sécurité**. Il conviendrait de garantir le respect des règles en matière de protection des données, par exemple en compartimentant les données et en instituant des règles distinctes en matière de contrôle d'accès pour chaque catégorie de données.

La constitution d'un répertoire commun de données permettrait de surmonter le problème actuel de la fragmentation de l'architecture européenne de gestion des données en matière de contrôle aux frontières et de sécurité. Cette fragmentation est contraire au principe de minimisation des données, car elle a pour conséquence le stockage multiple de données identiques. Si nécessaire, le répertoire commun permettrait de reconnaître les connexions et de fournir une image globale en combinant divers éléments d'information stockés dans différents systèmes d'information. Il pallierait, ce faisant, les insuffisances actuelles en matière d'information et permettrait aux garde-frontières et aux agents de police d'obtenir des éclaircissements sur certaines zones d'ombre.

***Schéma n° 5** Répertoire commun de données*



La solution consistant à constituer un répertoire commun de données au niveau de l'UE soulève d'importantes questions relatives à la définition de la finalité, de l'utilité, de la faisabilité technique et de la proportionnalité du traitement de données induit. Elle nécessiterait une révision complète du cadre juridique régissant les différents systèmes d'information, objectif qui ne saurait être atteint qu'à long terme. Le groupe d'experts sur les systèmes d'information et l'interopérabilité examinera les aspects juridiques, techniques et opérationnels liés à la constitution d'un répertoire commun de données, y compris les aspects de protection des données.

Pour les quatre dimensions de l'interopérabilité susmentionnées (interface de recherche unique, interconnexion des systèmes, service partagé de mise en correspondance de données biométriques et répertoire commun de données), il est nécessaire que les données stockées dans les différents systèmes ou modules d'information soient compatibles entre elles. Pour y parvenir, il importe de poursuivre les travaux sur un **format de message uniforme** (UMF) afin de créer une norme commune à l'ensemble des systèmes d'information pertinents[28].

Actions pour l'interopérabilité des systèmes d'information

- La Commission créera un **groupe d'experts sur les systèmes d'information et l'interopérabilité,** avec les agences de l'UE, les États membres et les parties prenantes concernées, afin d'examiner les aspects juridiques, techniques et opérationnels du renforcement de l'interopérabilité des systèmes d'information, notamment l'utilité, la faisabilité technique et la proportionnalité des options disponibles et leurs conséquences sur le plan de la protection des données.

Interface de recherche unique

- La Commission et l'eu-LISA aideront les États membres à installer une interface de recherche unique pour interroger les systèmes centraux.
- La Commission et l'eu-LISA examineront, avec le groupe d'experts, si des interfaces de recherche uniques peuvent être utilisées pour effectuer simultanément, dans le cadre d'un guichet unique, des recherches dans tous les systèmes pertinents, sans modifier les droits d'accès actuels.

Interconnexion des systèmes d'information

- La Commission et l'eu-LISA examineront, avec le groupe d'experts, la possibilité de promouvoir encore l'interconnexion entre les systèmes d'information centralisés, au-delà de l'interconnexion déjà proposée entre le système d'entrée/sortie et le système d'information sur les visas.

Service de mise en correspondance de données biométriques

- La Commission et l'eu-LISA examineront, avec le groupe d'experts, l'utilité et la faisabilité technique de la mise en place d'un service partagé de mise en correspondance de données biométriques pour tous les systèmes d'information pertinents.

[28] La Commission a approuvé la poursuite du développement de l'UMF dans sa communication de 2012 sur le modèle européen d'échange d'informations (EIXM) et finance actuellement le troisième projet pilote sur l'UMF, dont l'objectif est de créer une norme commune à l'ensemble des bases de données pertinentes, à utiliser aux niveaux national (États membres), de l'UE (systèmes centraux et agences) et international (Interpol).

Répertoire commun de données (module central)

- La Commission et l'eu-LISA examineront, avec le groupe d'experts, les conséquences juridiques, techniques, opérationnelles et financières de l'élaboration à long terme d'un répertoire commun de données.
- La Commission et l'eu-LISA participeront aux travaux en cours visant à créer un format de message uniforme global couvrant l'ensemble des systèmes d'information pertinents.

8. CONCLUSION

La présente communication engage une réflexion sur la manière dont les systèmes d'information de l'UE peuvent contribuer à renforcer la gestion des frontières et la sécurité intérieure, en s'appuyant sur les synergies importantes entre le programme européen en matière de sécurité et l'agenda européen en matière de migration. Un certain nombre de systèmes d'information fournissent déjà des informations pertinentes aux garde-frontières et aux agents de police, mais ils présentent des lacunes. L'UE doit relever le défi qui consiste à construire une architecture de gestion des données plus robuste et plus intelligente, dans le plein respect des droits fondamentaux, en particulier pour ce qui est de la protection des données à caractère personnel et du principe y afférent de la limitation des finalités.

Les lacunes de l'architecture de gestion des données de l'UE doivent être comblées. Conjointement avec la présente communication, la Commission a présenté une proposition relative à un système d'entrée/sortie qui devrait être adoptée d'urgence. La directive sur les données des dossiers passagers doit également être adoptée dans les prochaines semaines. La proposition relative à la création d'un corps européen de garde-frontières et de garde-côtes devrait être adoptée avant l'été. En parallèle, la Commission continuera à œuvrer au renforcement et, le cas échéant, à la rationalisation des systèmes existants, tels que la mise en place d'un système automatisé d'identification des empreintes digitales pour le système d'information Schengen.

Les États membres doivent tirer pleinement parti des systèmes d'information existants et établir les connexions techniques nécessaires à l'ensemble des systèmes d'information et bases de données, dans le respect de leurs obligations légales. Il convient de remédier au plus vite aux lacunes existantes, notamment dans le cadre Prüm. La présente communication lance un débat et engage un processus visant à combler les lacunes et les défaillances systémiques, mais il incombe aux États membres de remédier de toute urgence aux insuffisances persistantes en ce qui concerne l'alimentation des bases de données de l'UE et l'échange d'informations dans l'ensemble de l'Union.

Afin d'améliorer de manière structurelle l'architecture de gestion des données de l'UE en matière de contrôle aux frontières et de sécurité, la présente communication engage un processus devant aboutir à l'interopérabilité des systèmes d'information. La Commission créera un groupe d'experts sur les systèmes d'information et l'interopérabilité chargé d'examiner les modalités juridiques, techniques et opérationnelles des différentes options permettant de parvenir à l'interopérabilité des systèmes d'information, ainsi que de remédier aux éventuelles insuffisances et lacunes. À la suite des conclusions du groupe d'experts, la Commission européenne présentera de nouvelles propositions concrètes au Parlement européen et au Conseil comme base de discussion conjointe sur la voie à suivre. Elle recueillera également les contributions du Contrôleur européen de la protection des données et des autorités nationales chargées de la protection des données qui se rassemblent au sein du groupe de travail «article 29».

L’objectif devrait être la mise au point d’une stratégie conjointe visant à rendre la gestion de données dans l’UE plus efficace et efficiente, dans le plein respect des exigences en matière de protection des données, afin de mieux protéger les frontières extérieures de l’UE et de renforcer sa sécurité intérieure, au profit de tous les citoyens.

ANNEXE 1: ABREVIATIONS

API	Informations préalables sur les passagers
AFIS	Système automatisé d'identification des empreintes digitales: système capable de relever, conserver, comparer et vérifier les empreintes digitales
SID	Système d'information douanier
ECRIS	Système européen d'information sur les casiers judiciaires
EES	Système (proposé) d'entrée/sortie
EIXM	Modèle européen d'échange d'informations
SIE	Système d'information Europol
EPRIS	Système d'index européen des registres de la police
EURODAC	Système européen de comparaison des empreintes digitales
EUROPOL	Office européen de police (autorité répressive de l'Union européenne)
ETIAS	Système (éventuel) de l'UE d'information et d'autorisation concernant les voyages
eu-LISA	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
FIND	Fixed Interpol Networked Database (Base de données en réseau fixe d'Interpol)
FRONTEX	Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne
iARMS	Système (Interpol) de gestion des données sur les armes illicites et du traçage des armes
INTERPOL	Organisation internationale de police criminelle
MIND	Mobile Interpol Networked Database (Base de données en réseau mobile d'Interpol)
UIP	Unité d'informations passagers: à créer dans chaque État membre pour que les transporteurs aériens puissent communiquer les données PNR
PNR	Dossier passager
Prüm	Mécanisme de coopération policière permettant d'échanger des informations en ce qui concerne l'ADN, les empreintes digitales et les données relatives à l'immatriculation des véhicules
SafeSeaNet	Plateforme européenne d'échange de données dans le domaine maritime entre les autorités maritimes des États membres
SBC	Code frontières Schengen
SIENA	Application de réseau d'échange sécurisé d'informations
SIS	Système d'information Schengen (parfois appelé «de 2e génération» – SIS II)
SLTD	Base de données (d'Interpol) sur les documents de voyage perdus ou volés
s-TESTA	Services télématiques transeuropéens sécurisés entre administrations [feront l'objet d'une mise à niveau: TESTA-NG (prochaine génération)]

UMF	Uniform Message Format (format de message uniforme): format de message visant à assurer la compatibilité entre les systèmes d'information
VIS	Système d'information sur les visas
DIV	Données relatives à l'immatriculation des véhicules

ANNEXE 2: INVENTAIRE DES SYSTEMES D'INFORMATION EXISTANTS EN MATIERE DE GESTION DES FRONTIERES ET DE CONTROLE DE L'APPLICATION DE LA LOI

1. Le système d'information Schengen (SIS)

Le SIS est la plateforme d'échange d'informations la plus importante et la plus largement utilisée en matière d'immigration et de contrôle de l'application de la loi. Il s'agit d'un système centralisé utilisé par 25 États membres de l'UE[29] et quatre pays associés à l'espace Schengen[30], qui contient à l'heure actuelle 63 millions de signalements. Ces derniers sont introduits et consultés par les autorités compétentes telles que la police, les autorités chargées des contrôles aux frontières et les services de l'immigration. Le système contient des données sur des ressortissants de pays tiers auxquels l'accès à l'espace Schengen ou le séjour dans celui-ci est interdit, ainsi que sur des ressortissants de l'UE et de pays tiers qui sont recherchés ou portés disparus (y compris des enfants) et sur des objets recherchés (armes à feu, véhicules, documents d'identité, équipement industriel, etc.). Ce qui différencie le SIS par rapport à d'autres instruments d'échange d'informations est le fait que ses informations sont complétées par une instruction relative à la conduite à tenir concrètement par les agents sur le terrain, comme procéder à une arrestation ou à une saisie.

Les vérifications dans le SIS sont obligatoires pour le traitement des demandes de visa de court séjour, pour les vérifications aux frontières appliquées aux ressortissants de pays tiers et, de manière non systématique[31], aux citoyens de l'UE et aux autres personnes jouissant du droit à la libre circulation. Par ailleurs, tout contrôle de police sur le territoire devrait inclure un contrôle automatique dans le SIS.

2. Système d'information sur les visas (VIS)

Le VIS est un système centralisé d'échange de données sur les visas de court séjour entre les États membres. Il traite les données et les décisions concernant les demandes de visa de court séjour pour se rendre dans l'espace Schengen ou y transiter. Tous les consulats des États faisant partie de l'espace Schengen (environ 2 000) et tous leurs points de passage des frontières extérieures (près de 1 800 au total) sont connectés à ce système.

Le VIS contient des données sur les demandes de visa et les décisions y afférentes et indique si les visas délivrés sont révoqués, annulés ou prorogés. Ces données concernent actuellement 20 millions de demandes de visa et le système effectue, lors des pics de demande, plus de 50 000 transactions par heure. Chaque demandeur de visa fournit des informations biographiques détaillées, une photo numérique et dix empreintes digitales. Cela constitue dès lors un moyen fiable pour vérifier l'identité des demandeurs de visa, évaluer les cas éventuels de migration irrégulière et les risques potentiels pour la sécurité, et pour prévenir la pratique dite du «visa shopping» (course au visa).

Aux points de passage frontaliers ou sur le territoire des États membres, le VIS est utilisé pour vérifier l'identité des titulaires de visas en comparant leurs empreintes digitales avec celles qui sont stockées dans le VIS. Cette procédure garantit que le demandeur de visa et la personne qui franchit la frontière ne sont qu'une seule et même personne. Une recherche d'empreintes digitales dans le VIS permet également d'identifier une personne

[29] L'ensemble des États membres, à l'exception de Chypre, de la Croatie et de l'Irlande.
[30] L'Islande, le Liechtenstein, la Norvège et la Suisse.
[31] Cette règle est susceptible d'être modifiée selon les modalités prévues par la proposition COM(2015) 670 de la Commission relative à la modification du code frontières Schengen.

qui a introduit une demande de visa au cours des cinq dernières années et qui n'est peut-être pas en possession de documents d'identité.

3. EURODAC

EURODAC (système européen de comparaison des empreintes digitales) contient les empreintes digitales des demandeurs d'asile et des ressortissants de pays tiers qui franchissent illégalement les frontières extérieures de l'espace Schengen. Son objectif principal à l'heure actuelle est de déterminer quel pays de l'UE est responsable du traitement d'une demande d'asile, conformément au règlement de Dublin. Ce système est disponible aux points de passage frontaliers, mais contrairement aux systèmes SIS et VIS, il ne s'agit pas d'un système de gestion des frontières.

Les empreintes digitales des migrants en situation irrégulière qui pénètrent illégalement sur le territoire de l'UE sont relevées aux points de passage frontaliers. Elles sont stockées dans EURODAC pour pouvoir vérifier l'identité de la personne en cas de future demande d'asile. Les services de l'immigration et les autorités policières peuvent également comparer les données dactyloscopiques des migrants en situation irrégulière se trouvant dans des États membres de l'UE afin de vérifier s'ils ont demandé l'asile dans un autre État membre. Les autorités répressives et Europol peuvent aussi consulter EURODAC en vue de prévenir ou de détecter des formes graves de criminalité ou des infractions terroristes, ou de mener des enquêtes en la matière.

L'enregistrement des empreintes digitales des demandeurs d'asile ou des migrants en situation irrégulière dans un système centralisé permet la détection et le suivi de leurs mouvements secondaires[32] au sein de l'UE, jusqu'à ce qu'une demande de protection internationale ait été présentée ou qu'une décision de retour ait été prise (à l'avenir, cela fera l'objet d'un signalement correspondant dans le SIS). De manière plus générale, l'identification et le suivi des migrants en situation irrégulière sont indispensables pour garantir la délivrance de nouveaux documents par les autorités de leur pays d'origine et, partant, pour faciliter le retour de ces personnes.

4. Base de données sur les documents de voyage perdus ou volés (SLTD)

La base de données d'Interpol sur les documents de voyage perdus ou volés (SLTD) est une base de données centrale sur les passeports et les autres documents de voyage dont le vol ou la perte ont été déclarés à Interpol par les autorités de délivrance. Elle contient des informations relatives aux passeports vierges volés. Les documents de voyage dont le vol ou la perte ont été déclarés aux autorités des pays participant au SIS sont répertoriés dans la base de données SLTD et dans le SIS. La base de données SLTD contient également des données relatives aux documents de voyage introduites par des pays ne participant pas au SIS (Chypre, Croatie, Irlande et pays tiers).

Ainsi qu'il est indiqué dans les conclusions du Conseil des 9 et 20 novembre 2015 et dans la proposition de règlement de la Commission du 15 décembre 2015 concernant une modification ciblée du code frontières Schengen[33], les documents de voyage de tous les ressortissants de pays tiers et de toutes les personnes jouissant du droit à la libre circulation doivent être vérifiés en consultant la base de données SLTD. Tous les postes

[32] Par exemple, dans le cas des réfugiés qui arrivent en Grèce et qui n'ont pas l'intention de présenter une demande d'asile dans ce pays, mais bien de poursuivre leur voyage vers d'autres États membres par voie terrestre.

[33] COM(2015) 670 final - proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 562/2006 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures.

de contrôle frontaliers doivent être reliés à cette base de données. Par ailleurs, les recherches effectuées à des fins répressives dans la base de données SLTD au niveau national auraient des effets positifs supplémentaires sur le plan de la sécurité.

5. Informations préalables sur les passagers (API)

L'objectif du système API est de recueillir des informations sur l'identité des personnes avant l'embarquement pour les vols à destination de l'UE et d'identifier les migrants en situation irrégulière à l'arrivée. Les données que contient le système sont les informations figurant dans un document de voyage, à savoir le nom complet du voyageur, sa date de naissance, sa nationalité, le numéro et le type du document de voyage, ainsi que des informations relatives au point de passage frontalier de départ et d'entrée et des précisions sur le transport. Les données API relatives aux passagers sont généralement recueillies au moment de l'enregistrement.

Les informations préalables à l'arrivée concernant les transports par voie maritime doivent être transmises 24 heures avant l'arrivée prévue du bateau, en vertu de la convention visant à faciliter le trafic maritime international. La directive 2010/65/UE[34] prévoit la transmission électronique des données au moyen d'un guichet unique reliant SafeSeaNet, e-Customs et d'autres systèmes électroniques.

Il n'existe aucun système central de l'UE permettant d'enregistrer les données API.

6. Système d'information Europol

Le système d'information Europol (SIE) est une base de données centralisée contenant des informations à caractère pénal à des fins d'enquête. Il peut être utilisé par les États membres et par Europol pour conserver les données relatives aux formes graves de criminalité et au terrorisme et pour effectuer des recherches en la matière. Les informations stockées dans le SIE sont des données relatives à des personnes, à des documents d'identité, à des voitures, à des armes à feu, à des numéros de téléphone, à des courriels, à des empreintes digitales, à l'ADN, ainsi qu'à la cybercriminalité; ces données peuvent être mises en rapport de différentes manières afin de donner une vue d'ensemble plus détaillée et structurée d'une affaire de criminalité. Le SIE soutient la coopération des services répressifs et ne peut être consulté par les autorités chargées des contrôles aux frontières.

L'échange d'informations s'effectue par l'intermédiaire de la plateforme SIENA[35], un réseau de communication électronique sécurisé entre Europol, les bureaux de liaison, les unités nationales Europol, les autorités compétentes désignées (telles que les douanes, les bureaux de recouvrement des avoirs, etc.) et les tiers concernés.

Un nouveau cadre juridique pour Europol entrera en vigueur en mai 2017. Il permettra de renforcer la capacité opérationnelle d'analyse d'Europol, ainsi que de mieux établir des liens entre les informations disponibles.

---

[34] Directive 2010/65/UE du Parlement européen et du Conseil du 20 octobre 2010 concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE.

[35] Application de réseau d'échange sécurisé d'informations.

7. Le cadre Prüm

Le cadre Prüm se fonde sur un accord multilatéral[36] entre les États membres qui permet l'échange de données relatives à l'ADN, aux empreintes digitales et à l'immatriculation des véhicules (DIV). Le concept repose sur l'interconnexion entre un système national et les systèmes nationaux de tous les autres États membres de l'UE, afin de permettre des consultations croisées à distance. Lorsqu'une recherche aboutit à une correspondance positive dans la base de données d'autres États membres, les détails de cette correspondance sont échangés au moyen de mécanismes d'échange bilatéraux.

8. Système européen d'information sur les casiers judiciaires (ECRIS)

L'ECRIS est un système électronique d'échange d'informations sur les condamnations antérieures prononcées par des juridictions pénales dans l'UE à l'encontre d'une personne déterminée, aux fins d'une procédure pénale à l'encontre d'une personne et, si la législation nationale l'autorise, à d'autres fins. L'État membre de condamnation doit notifier les condamnations pénales prononcées à l'encontre d'un ressortissant d'un autre État membre à l'État membre de nationalité de la personne concernée. L'État membre de nationalité doit conserver ces informations et est donc en mesure de fournir, sur demande, des informations à jour sur le casier judiciaire de ses ressortissants, quel que soit le lieu où les condamnations ont été prononcées dans l'Union européenne.

L'ECRIS permet également l'échange d'informations sur les condamnations pénales prononcées à l'encontre de ressortissants de pays tiers et de personnes apatrides. Les autorités centrales désignées dans chaque État membre constituent les points de contact du réseau ECRIS, prenant en charge toutes les tâches telles que la notification, la conservation, la demande et la fourniture d'informations sur les casiers judiciaires.

[36] Traité de Prüm (2005), intégré dans la législation de l'UE en 2008 par la décision 2008/615/JAI du Conseil.