Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

20.xxx

Message concernant l'approbation et la mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des règlements (UE) 2019/817 et (UE) 2019/818 relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (Développements de l'acquis de Schengen)

du 2 septembre 2020

Madame la Présidente,
Monsieur le Président,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet d'un arrêté fédéral portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des règlements (UE) 2019/817 et (UE) 2019/818 relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (développements de l'acquis de Schengen), en vous proposant de l'adopter.

Nous vous prions d'agréer, Madame la Présidente, Monsieur le Président, Mesdames, Messieurs, l'assurance de notre haute considération.

…

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Simonetta Sommaruga
Le chancelier de la Confédération, Walter Thurnherr

Condensé

L'interopérabilité des systèmes d'information de l'UE consistera à relier les différents systèmes entre eux. Il permettra aux autorités de contrôle aux frontières, de migration et de poursuite pénale d'obtenir en une seule requête des informations détaillées provenant de tous les systèmes d'information pertinents. L'identification des personnes sera par ailleurs facilitée grâce à la possibilité de comparer des données biométriques provenant de différents systèmes d'information. Les autorités pourront ainsi détecter les cas d'identités multiples et de fraude à l'identité. L'interopérabilité vise à améliorer la sécurité en Suisse et dans l'espace Schengen, à rendre les contrôles plus efficaces aux frontières extérieures et à contribuer à la gestion de la migration. Les droits d'accès des autorités compétentes ne seront pas étendus ni modifiés avec l'introduction de l'interopérabilité. Le présent message expose les mesures juridiques nécessaires à la reprise et à la mise en œuvre au niveau de la loi des deux règlements de l'UE sur l'interopérabilité et donne un aperçu des conséquences sur la Confédération et les cantons.

Contexte

Les autorités de contrôle aux frontières, de migration et de poursuite pénale ont accès à de nombreux systèmes d'information de l'UE. Ces systèmes ne sont cependant pas reliés entre eux. Il faut donc les consulter séparément afin d'obtenir des informations sur une personne et les synergies ne sont pas exploitées. Grâce à l'interopérabilité, les systèmes d'information de l'UE seront reliés entre eux de façon à pouvoir utiliser de manière plus efficace et plus ciblée les informations qui y sont enregistrées. À l'avenir, les autorités concernées pourront mener une recherche simultanément dans plusieurs systèmes d'information, dans la mesure où elles disposent des droits d'accès nécessaires aux systèmes en question. Ces droits ne sont ni étendus ni modifiés avec l'introduction de l'interopérabilité : celle-ci permet uniquement de reconnaître les données existantes et de les relier entre elles.

Contenu du projet

L'interopérabilité est assurée par la création d'un portail de recherche européen, qui permettra de consulter simultanément tous les systèmes d'information pertinents. Elle permet l'enregistrement centralisé des données d'identité et des données biométriques (empreintes digitales et images du visage) de ressortissants d'États tiers dans un répertoire commun et la comparaison automatique des données biométriques d'une personne, ce qui augmente les chances

En permettant une utilisation plus efficace des informations existantes, l'interopérabilité devrait renforcer la sécurité dans l'espace Schengen et en Suisse et améliorer la gestion de la migration. Ainsi, l'interopérabilité contribue à la réalisation des objectifs du Conseil fédéral pour 2020 dans les domaines de la sécurité et de la migration. La Suisse est confrontée à des défis transnationaux dans les domaines de la lutte contre la criminalité et de la gestion de la migration. Une coopération étroite et un échange rapide d'informations avec les autres États Schengen sont

essentiels pour les autorités suisses. L'interopérabilité permettra aux autorités suisses de contrôle aux frontières, de migration et de poursuite pénale d'identifier plus facilement les personnes qui représentent une menace pour la sécurité ou qui fournissent de fausses informations sur leur identité.

La mise en œuvre des deux règlements de l'UE (développements de l'acquis de Schengen) implique de modifier la loi fédérale sur les étrangers et l'intégration, la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile, la loi sur la responsabilité et la loi fédérale sur les systèmes d'information de police de la Confédération.

La transposition des règlements de l'UE sur l'interopérabilité entraînera une augmentation des charges financières et des charges de personnel pour l'administration fédérale et pour les cantons. Les systèmes d'information et les processus existants en Suisse doivent être adaptés afin de pouvoir profiter des possibilités qu'offre l'interopérabilité.

Table des matières

Condensé **2**

1 Introduction **7**

2 Contexte **7**

2.1 Nécessité d'agir et objectifs 7

2.2 Déroulement des négociations 10

2.3 Procédure de reprise des développements de l'acquis de Schengen 11

2.4 Relation avec le programme de la législature et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral 13

3 Procédure de consultation **13**

3.1 Condensé 13

3.2 Avis détaillés 14

4 Principes généraux des règlements de l'UE **18**

4.1 Vue d'ensemble 18

4.2 Applicabilité échelonnée des règlements sur l'interopérabilité 21

5 Contenu des règlements de l'UE **21**

5.1 Les quatre nouveaux composants centraux 22

5.1.1 Portail de recherche européen (ESP) (chap. II) 23

5.1.2 Service partagé d'établissement de correspondances biométriques (sBMS) (chap. III) 25

5.1.3 Répertoire commun de données d'identité (CIR) (chap. IV) 26

5.1.4 Détecteur d'identités multiples (MID) (chap. V) 29

5.2 Autres dispositions 35

6 Présentation de l'acte de mise en œuvre **39**

6.1 Réglementation proposée 39

6.2 Nécessité des adaptations proposées 39

6.3 Besoin particulier de coordination 43

7 Commentaire des dispositions de l'acte de mise en œuvre **44**

7.1 Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI) 44

7.2 Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA) 59

7.3 Loi du 14 mars 1958 sur la responsabilité (LRCF) 59

7.4 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP) 60

8 Besoins de coordination **65**

8.1 Coordination avec le projet d'arrêté fédéral ETIAS 65

8.2 Coordination avec la modification de la LEI du 14 décembre 2018 relative à la mise en œuvre des normes procédurales et des systèmes d'information 66
8.3 Coordination avec le projet d'arrêté fédéral SIS 66
8.4 Coordination avec le projet d'arrêté fédéral EES 67

9 Conséquences 67
9.1 Conséquences financières et conséquences sur l'état du personnel pour la Confédération 67
9.1.1 Conséquences financières et conséquences sur l'état du personnel: phase de projet 67
9.1.2 Conséquences financières et conséquences sur l'état du personnel: mise en service 69
9.2 Conséquences pour les cantons 72
9.2.1 Conséquences financières et conséquences sur l'état du personnel73
9.2.2 Plateforme de recherche nationale 73
9.3 Conséquences dans d'autres domaines 74

10 Aspects juridiques 74
10.1 Constitutionnalité 74
10.2 Compatibilité avec les obligations internationales de la Suisse 74
10.3 Forme de l'acte à adopter 75
10.4 Frein aux dépenses 75

Liste des abréviations utilisées 76

Arrêté fédéral

portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des règlements (UE) 2019/817 et (UE) 2019/818 relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE

(Développements de l'acquis de Schengen) *(projet)*

Échange de notes du 19 juin 2019[1] entre la Suisse et l'Union européenne concernant la reprise du règlement (UE) 2019/817 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 et les décisions 2004/512/CE et 2008/633/JAI

Échange de notes du 19 juin 2019[2] entre la Suisse et l'UE concernant la reprise du règlement (UE) 2019/818 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816

1 RS **0.362.380.xxx**; RO **xxxxx**
2 RS **0.362.380.xxx**; RO **xxxxx**

Message

1 Introduction

L'objectif de l'interopérabilité est d'améliorer la sécurité en Suisse et dans l'espace Schengen, de permettre des contrôles plus efficaces aux frontières extérieures et de contribuer à la gestion de la migration. Pour ce faire, l'interopérabilité relie entre eux les systèmes d'information actuels de l'UE en matière de coopération Schengen-Dublin, de manière à ce que les données d'identité, les données des documents de voyage et les données biométriques (empreintes digitales et images du visage) puissent être comparées automatiquement. Ainsi, les informations disponibles pourront être consultées plus facilement et plus rapidement. Il en résulte un renforcement de la sécurité ainsi qu'une meilleure gestion de la migration. Les autorités de poursuite pénale, de contrôle aux frontières et de migration bénéficieront toutes de l'interopérabilité. Leurs droits d'accès aux différents systèmes d'information restent identiques. Le présent message porte sur la reprise et la mise en œuvre des règlements (UE) 2019/817[3] et (UE) 2019/818[4] relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police.

2 Contexte

2.1 Nécessité d'agir et objectifs

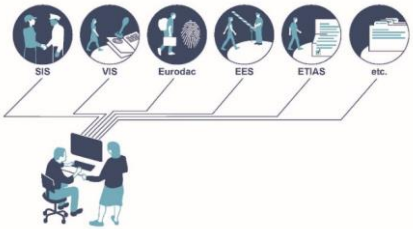
Les autorités de contrôle aux frontières, de migration et de poursuite pénale ont déjà accès à différents systèmes d'information de l'UE. Cependant, ces systèmes ne sont pas reliés entre eux du point de vue technique: les données sont enregistrées séparément dans les différents systèmes d'information. Les synergies ne peuvent donc pas être exploitées et des informations et des concordances importantes risquent de ne pas être découvertes lorsque le système dans lequel les données sont enregistrées n'est pas consulté directement. Des autorités pourraient ainsi passer à côté d'informations pertinentes. L'exemple ci-après illustre l'une des failles importantes existant actuellement. L'interopérabilité permettra de la combler.

3 Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, version du JO L 135 du 22.5.2019, p. 27.

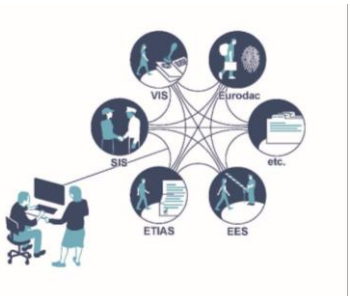
4 Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816, version du JO L 135 du 22.5.2019, p. 85.

Un criminel provenant d'un État tiers a fait l'objet d'un signalement en Suisse dans le Système d'information Schengen (SIS) en vue d'une interdiction d'entrée et a été renvoyé dans son pays d'origine. Il demande par la suite un visa auprès de l'ambassade d'un autre État Schengen sous une fausse identité. Ses empreintes digitales sont certes enregistrées dans le système central d'information sur les visas (VIS), mais elles ne sont pas comparées avec les empreintes enregistrées dans le SIS. Il obtient un visa et réussit ainsi à revenir dans l'espace Schengen.

Grâce à l'interopérabilité entre les systèmes d'information de l'UE, les données d'identité, les données des documents de voyage et les données biométriques (empreintes digitales et images du visage) de ressortissants d'États tiers seront désormais comparées automatiquement. Ainsi, les criminels qui opèrent sous une fausse identité pourront être identifiés. Tous les systèmes d'information (en l'occurrence, le SIS et le VIS) pourront être consultés en même temps et en une seule requête.



Sans l'interopérabilité, chaque système devrait être consulté séparément.



Avec l'interopérabilité, les autorités pourront consulter tous les systèmes d'informations en même temps et en une seule requête.

Assurer l'interopérabilité signifie donc relier les systèmes d'information de l'UE entre eux afin de pouvoir utiliser de manière plus efficace et plus ciblée les informations qui y sont enregistrées. À l'avenir, les autorités compétentes pourront obtenir toutes les informations pertinentes pour leurs tâches concernant une personne et se faire rapidement une idée complète. Le but est que les autorités disposent toujours des informations dont elles ont besoin, pour éviter par exemple d'octroyer un visa à un criminel issu d'un État tiers. À cette fin, le Parlement européen et le Conseil de l'Union européenne ont adopté, le 20 mai 2019, deux règlements visant l'établissement de l'interopérabilité entre les systèmes d'information de l'UE :

– le règlement (UE) 2019/817[5], qui concerne les domaines des frontières et des visas (ci-après « règlement IOP Frontières »);

– le règlement (UE) 2019/818[6], qui concerne les domaines de la coopération policière et judiciaire, de l'asile et de l'immigration (ci-après « règlement IOP Police »).

Ces deux règlements prévoient la création des composants suivants:

- le portail de recherche européen (*European Search Portal*, ESP), qui permettra aux autorités compétentes d'effectuer une recherche simultanée dans plusieurs systèmes d'information;
- le service partagé d'établissement de correspondances biométriques (*shared Biometric Matching Service*, sBMS), qui permettra de comparer des données biométriques (empreintes digitales et images du visage) provenant de plusieurs systèmes;
- le répertoire commun de données d'identité (*Common Identity Repository*, CIR), qui contiendra les données d'identité de ressortissants d'États tiers, les données de leurs documents de voyage et leurs données biométriques provenant de divers systèmes d'information de l'UE;
- le détecteur d'identités multiples (*Multiple Identity Detector*, MID), qui permettra de détecter les liens entre les données des différents systèmes raccordés entre eux (liens MID) et de démasquer les personnes utilisant une fausse identité ou des identités multiples.

Assurer l'interopérabilité revient non pas à collecter de nouvelles données, mais uniquement à créer de nouvelles fonctions pour les systèmes d'information actuels et futurs (SIS, VIS, système d'entrée et de sortie [EES], système européen d'information et d'autorisation concernant les voyages [ETIAS], banque de données centrale de l'Union européenne contenant les empreintes digitales de personnes qui ont déposé une demande d'asile dans un État Dublin et ont été appréhendées lors de leur entrée illégale [Eurodac]). Rien ne change donc pour les autorités en ce qui

5 Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, version du JO L 135 du 22.5.2019, p. 27.

6 Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816, version du JO L 135 du 22.5.2019, p. 85.

concerne les droits d'accès aux systèmes d'information sous-jacents.

Les deux règlements de l'UE sur l'interopérabilité ont été élaborés à la suite des attentats commis depuis 2015 dans l'espace Schengen et en réponse aux défis croissants dans le domaine migratoire. Le développement et l'élargissement des structures informatiques de l'UE constituent des éléments centraux de l'amélioration de la sécurité dans l'espace Schengen. L'interopérabilité des systèmes d'information de l'UE joue un rôle important pour combler les lacunes en matière de sécurité. L'échange facilité des données doit aussi permettre de mener des contrôles plus rapides et plus efficaces aux frontières extérieures et de soutenir la lutte contre la migration irrégulière. L'objectif est de pouvoir utiliser de manière plus efficace et plus ciblée les informations déjà disponibles, ce qui représente une importante plus-value pour le travail des autorités de poursuite pénale, de contrôle aux frontières et de migration.

En signant l'accord d'association à Schengen (AAS)[7], la Suisse s'est engagée à reprendre tous les développements de l'acquis de Schengen (art. 2, al. 3, et 7 AAS). La reprise d'un nouvel acte juridique a lieu dans le cadre d'une procédure spéciale qui inclut la notification par les organes compétents de l'UE du développement à reprendre et la transmission d'une note de réponse de la part de la Suisse.

Les deux règlements ont été notifiés à la Suisse le 21 mai 2019 en tant que développements de l'acquis de Schengen. Le 14 juin 2019, le Conseil fédéral a adopté les échanges de notes concernant la reprise des règlements sous réserve de l'approbation du Parlement. La note de réponse a été transmise à l'UE le 19 juin 2019. Le présent projet vise à reprendre les développements de l'acquis de Schengen dans les délais impartis et à créer les bases légales nécessaires à leur mise en œuvre. Pour ce faire, la Suisse dispose d'un délai de deux ans au maximum et celui-ci arrive à échéance le 21 mai 2021.

2.2 Déroulement des négociations

Le 12 décembre 2017, la Commission européenne a présenté les deux propositions de règlement sur l'interopérabilité, qui forment ensemble les bases légales pour l'établissement de l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police. Les débats au sein du Conseil de l'UE ont duré de janvier à septembre 2018, puis les négociations avec le Parlement européen (trilogue) d'octobre 2018 à février 2019. Les représentants de la Suisse ont participé à toutes les réunions et ont pu clarifier des questions techniques et apporter leurs propositions de solutions à toutes les étapes de la négociation.

Les sujets suivants ont donné lieu à des discussions particulièrement intenses:

7 Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen; RS **0.362.31**.

- Mise en œuvre: outre les conséquences financières pour les États Schengen, il a été question des effets de la mise en œuvre sur les contrôles des personnes aux frontières extérieures de Schengen ; des doutes ont été exprimés en particulier sur la faisabilité technique d'une consultation simultanée de tous les systèmes interopérables lors de contrôles de personnes aux frontières extérieures ;
- Besoins accrus en personnel: la question de l'augmentation des coûts de personnel pour les États Schengen a été abordée à plusieurs reprises, de même que la charge supplémentaire pour les services existants tels que les bureaux nationaux SIRENE, qui sont responsables de l'échange d'informations et de la coordination de la procédure en cas de réponse positive dans le SIS ;
- Géométrie variable: ce terme recouvre la problématique de la non-participation de certains États à un ou plusieurs systèmes d'information de l'UE, les différences dans le degré d'intégration conduisant à des résultats de recherches variables dans les systèmes centraux interopérables ; la question concerne surtout, à l'heure actuelle, le Royaume-Uni et l'Irlande, qui n'ont pas accès au SIS et qui ne peuvent donc pas profiter des fonctionnalités du MID permettant de détecter les identités multiples, mais aussi la Suisse et d'autres États associés en raison de l'accès limité aux données de l'Office européen de police (Europol) ou de l'absence d'accès au système européen d'information sur les casiers judiciaires (ECRIS-TCN) pour les ressortissants d'États tiers.
- Consultation des banques de données de l'Organisation internationale de police criminelle (Interpol): la base légale d'une consultation des banques de données d'Interpol en tant qu'élément de l'interopérabilité continue de faire l'objet de discussions ; il est prévu de régler les questions ouvertes dans le cadre d'un accord entre l'UE et Interpol.
- Autres thèmes : l'accès au CIR à des fins d'identification ou de poursuite pénale et l'information aux ressortissants d'États tiers concernés.

Le compromis obtenu a été accepté lors de la session plénière du Parlement européen le 16 avril 2019 et par le Conseil des ministres le 14 mai 2019. Les règlements ont été adoptés formellement le 20 mai 2019 lors de la signature de l'acte juridique afférent par les présidents du Parlement européen et du Conseil de l'UE. Le développement de l'acquis de Schengen a été notifié à la Suisse le 21 mai 2019.

2.3 Procédure de reprise des développements de l'acquis de Schengen

Conformément à l'art. 2, par. 3, AAS, la Suisse s'est engagée à reprendre tout acte juridique édicté par l'UE en tant que développement de l'acquis de Schengen depuis la signature de l'AAS le 26 octobre 2004 et, si nécessaire, à le transposer dans le droit suisse.

L'art. 7 AAS prévoit une procédure spéciale pour la reprise et la mise en œuvre des développements de l'acquis de Schengen. En premier lieu, l'UE notifie « sans délai » à la Suisse l'adoption d'un acte constituant un développement de l'acquis de Schengen. Le Conseil fédéral dispose ensuite d'un délai de 30 jours pour indiquer à l'institution européenne compétente (Conseil de l'UE ou Commission) si la Suisse

reprendra ou non le développement et, le cas échéant, dans quel délai. Le délai de 30 jours commence à courir à la date de l'adoption de l'acte juridique par l'UE (art. 7, par. 2, AAS).

Si l'acte en question est juridiquement contraignant, la notification par l'UE et la note de réponse de la Suisse constituent un échange de notes qui représente, du point de vue de la Suisse, un traité de droit international. Conformément aux dispositions constitutionnelles, ce traité doit être approuvé soit par le Conseil fédéral, soit par le Parlement et, en cas de référendum, par le peuple.

Les deux règlements soumis à la Suisse sont juridiquement contraignants. Aussi doivent-ils faire l'objet d'un échange de notes.

En l'espèce, l'approbation de l'échange de notes relève de la compétence de l'Assemblée fédérale (cf. ch. 10.1). La Suisse a donc notifié à l'UE, dans ses deux notes de réponse du 19 juin 2019, qu'elle ne pourra, sur le plan juridique, être liée par le développement en question qu'« après l'accomplissement de ses exigences constitutionnelles » (art. 7, par. 2, let. b, AAS). Le délai maximal dont dispose alors la Suisse pour la reprise et la mise en œuvre du développement est de 2 ans à compter de la notification des actes en question par le Conseil de l'UE, y compris pour l'organisation d'une votation en cas d'aboutissement d'une demande de référendum.

Dès que la procédure nationale a pris fin et que toutes les exigences constitutionnelles liées à la reprise et à la mise en œuvre des deux règlements européens ont été accomplies, la Suisse informe sans délai par écrit le Conseil de l'UE et la Commission. Si aucune demande de référendum n'est lancée contre la reprise et la mise en œuvre de ces règlements, la Suisse communique cette information, assimilée à la ratification des échanges de notes, au Conseil de l'UE ainsi qu'à la Commission dès l'échéance du délai référendaire.

Si la Suisse ne met pas en œuvre un développement de l'acquis de Schengen dans les délais impartis, elle risque la fin de la coopération Schengen dans son ensemble, et donc également la fin de la coopération Dublin (art. 7, par. 4, AAS, en relation avec l'art. 14, par. 2, AAD[8]).

Sur la base de la date de notification de l'UE (21 mai 2019), le délai maximal de 2 ans pour la reprise et la mise en œuvre des règlements de l'UE arrive à échéance le 21 mai 2021. Étant donné que la mise en service des composants de l'interopérabilité, et partant le début de l'application des dispositions concernées dans les règlements, sont prévus pour une date ultérieure (pour les détails, cf. ch. 4.2), le pragmatisme devrait néanmoins permettre de disposer *de facto* d'une certaine marge de manœuvre pour dépasser légèrement les délais. C'est bien le cas pour les règlements de l'UE sur l'interopérabilité, puisque les différents composants seront mis en service de manière échelonnée et que la mise en œuvre complète n'est pas prévue avant 2023.

8 Accord du 26 octobre 2004 entre la Confédération suisse et la Communauté européenne relatif aux critères et aux mécanismes permettant de déterminer l'État responsable de l'examen d'une demande d'asile introduite dans un État membre ou en Suisse; RS **0.142.392.68**

2.4 Relation avec le programme de la législature et avec le plan financier, ainsi qu'avec les stratégies du Conseil fédéral

L'adoption du présent message est l'un des objectifs annuels du Conseil fédéral pour 2020. Le projet a été annoncé dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[9].

En utilisant de manière optimale et interopérable les différents systèmes d'information de l'UE, la Suisse développera ses relations politiques et économiques avec l'UE. Le fait de mettre rapidement et complètement les informations pertinentes à la disposition des autorités compétentes contribue à la réalisation des objectifs de gestion de la migration et de lutte contre la migration irrégulière. La Suisse doit prévenir la violence, la criminalité et le terrorisme et lutter efficacement contre ces phénomènes. Elle doit connaître les menaces contre la sécurité et posséder les instruments nécessaires pour y faire face efficacement. L'interopérabilité soutient ce travail en permettant une utilisation plus efficace des systèmes d'information de l'UE.

Une première tranche du crédit d'engagement « Développements Schengen/Dublin » destinée à la réalisation de l'interopérabilité des systèmes d'information de l'UE figure au budget 2020 assorti d'un plan intégré des tâches et des finances pour les années 2021 à 2023. Une fois que les plans de gestion de projet mis à jour et qu'un rapport sur la qualité des projets concernés et sur les risques qu'ils présentent seront disponibles, le Conseil fédéral libérera la deuxième tranche du crédit d'engagement. Tous les moyens ne peuvent être libérés que si l'Assemblée fédérale a adopté les bases légales.

La reprise et la mise en œuvre des règlements de l'UE sur l'interopérabilité n'entrent en conflit avec aucune stratégie du Conseil fédéral et sont adaptées pour remplir les obligations de la Suisse découlant de l'AAS.

3 Procédure de consultation

3.1 Condensé

Du 9 octobre 2019 au 9 janvier 2020, une consultation a été menée conformément à l'art. 3, al. 1, let. c, de la loi du 18 mars 2005 sur la consultation[10].

Tous les cantons, 3 partis politiques, 5 associations faîtières, le Tribunal administratif fédéral et 9 milieux intéressés y ont répondu, pour un total de 44 prises de position. Sur ces participants à la consultation, 7 ont renoncé expressément à formuler un avis.

9 FF **2020** 1709 1828
10 RS **172.061**

Dans le détail, 32 participants sont favorables au projet, 11 n'ont fait aucune remarque et 3 demandent des améliorations dans la mise en œuvre. Les résultats de la procédure de consultation sont présentés dans le rapport prévu à cet effet[11].

De nombreux cantons (AI, FR, GE, JU, LU, NE, OW, SH, SO, TI, VS et ZG), de même que l'Association des services cantonaux de migration (ASM), ont souligné que le projet entraînait des coûts et du travail supplémentaires, même si certains d'entre eux (AI, LU, VS et ASM) ont estimé que la plus-value sécuritaire qu'apporte l'interopérabilité est prépondérante. Les cantons du Jura et du Tessin ont demandé que le Conseil fédéral informe plus clairement les cantons de l'étendue des coûts et du travail supplémentaire à anticiper. Les cantons d'Obwald et de Genève ont demandé que la Confédération indemnise ou soutienne financièrement les cantons. Le PLR et l'UDC ont escompté recevoir des informations plus précises sur la faisabilité, la mise en œuvre et le financement de l'interopérabilité avant les délibérations parlementaires.

Si plusieurs organisations (Organisation suisse d'aide aux réfugiés [OSAR], Union syndicale suisse [USS], AsyLex et PS) se sont déclarées favorables à la reprise de ces développements de l'acquis de Schengen, qui garantiront que la Suisse puisse rester membre de Schengen-Dublin, elles ne se montrent pas moins critiques à l'égard du projet, une partie d'entre elles se déclarant favorable à un renforcement des droits fondamentaux et de la protection des données.

Au vu des avis exprimés, majoritairement positifs, l'arrêté fédéral n'a pas été modifié. Les préoccupations des participants à la consultation sont examinées plus en détail ci-après.

3.2 Avis détaillés

Protection des données

Plusieurs participants à la consultation ont critiqué le fait que les garanties concernant les droits fondamentaux et la protection des données des ressortissants d'États tiers sont à leurs yeux insuffisantes. Par ailleurs, ils redoutent les attaques de pirates informatiques. C'est pourquoi plusieurs d'entre eux ont demandé la mise en place de contrôles obligatoires par l'État et de prescriptions en matière de protection des données. En raison des tâches supplémentaires incombant aux autorités de surveillance de la protection des données, quelques-uns ont demandé une hausse des effectifs auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT) et des autorités cantonales de surveillance de la protection des données, voire un développement de leur structure organisationnelle.

11 L'ensemble des documents relatifs à la procédure de consultation peuvent être consultés à l'adresse suivante : www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2019 > DFJP

Le PS a proposé de créer un nouvel art. 111*k* LEI, qui prévoirait que le PFPDT publie chaque année, en tant qu'autorité de surveillance compétente à l'échelle nationale, le nombre de demandes de rectification ou d'effacement de données à caractère personnel, de même que le nombre de rectifications, d'effacements ou de limitations des données à caractère personnel effectivement opérés. Cet article préciserait par ailleurs les modalités d'établissement des rapports du PFPDT au Contrôleur européen de la protection des données (CEPD), aux autres autorités nationales de surveillance et au Parlement suisse. Enfin, il chargerait le Conseil fédéral de veiller à ce que le PFPDT dispose de ressources suffisantes pour accomplir ces tâches.

À cet égard, le Conseil fédéral relève que les deux règlements de l'UE sur l'interopérabilité des systèmes d'information, qui ont été élaborés avec la participation du CEPD, consacrent un chapitre entier à la protection des données et à sa surveillance (cf. chap. VII de ces règlements). Ils prévoient aussi un contrôle par le CEPD. Le chapitre 14*c* P-LEI contient par ailleurs désormais toutes les dispositions relatives à la protection des données dans le cadre de l'accord d'association à Schengen. Les principes de la législation sur la protection des données sont applicables, si bien que l'accès aux données doit être proportionné aux objectifs poursuivis et ne saurait être accordé que dans la mesure où les données consultées sont nécessaires pour permettre aux autorités compétentes d'accomplir leurs tâches. Pour juger du respect de la législation sur la protection des données, il est également essentiel que les droits d'accès des autorités aux systèmes d'information concernés par l'interopérabilité ne soient pas étendus. Or ces droits restent régis par les bases légales spécifiques à ces systèmes d'information.

Dans la mesure où les données sont consultées et traitées à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuite en la matière ou d'exécution de sanctions pénales, les dispositions de la directive (UE) 2016/680[12] s'appliquent; ces dispositions sont intégrées au droit suisse dans la loi fédérale du 28 septembre 2018 sur la protection des données Schengen (LPDS)[13]. Si le traitement des données vise d'autres fins, les règlements de l'UE sur l'interopérabilité exigent l'application du règlement général sur la protection des données (règlement [UE] 2016/679)[14]. Ce dernier n'est certes pas directement contraignant pour la Suisse, l'UE ne l'ayant pas classé comme relevant de Schengen et la Suisse, par conséquent, ne l'ayant pas repris dans sa législation en tant que développement de l'acquis de Schengen. Toutefois, dans le cadre de la coopération instaurée par

12 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.

13 RS **235.3**

14 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, JO 119 du 4.5.2016, p. 1.

Schengen, les prescriptions en matière de traitement des données de cet acte européen sont *indirectement* pertinentes pour la Suisse. Du reste, elles sont prises en compte dans la révision totale en cours de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[15]. L'objectif de la révision complète de la LPD est d'établir, en Suisse, un niveau de protection équivalent à celui prévu par la législation européenne, tant dans le domaine privé que dans le secteur public[16]. C'est pourquoi une mise en œuvre spécifique du règlement général sur la protection des données est superflue dans le cadre du présent projet.

Les enregistrements figurant dans les composants assurant l'interopérabilité sont soumis aux mêmes normes – élevées – de protection des données que ceux des systèmes d'information sous-jacents. Les autorités des États Schengen-Dublin qui sont responsables du traitement des données dans le sBMS et le CIR sont les mêmes que celles auxquelles incombe le traitement des données du SIS, du VIS et de l'EES. Le traitement des données contenues dans le MID relève de la compétence des services centraux d'ETIAS et des autorités des États Schengen-Dublin habilitées à ajouter ou modifier des données dans le dossier de confirmation d'identité. La responsabilité de la sécurité des composants centraux et des infrastructures de communication incombe à l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), qui assure le retour à un fonctionnement normal en cas de panne ou de dérangement, par exemple.

S'agissant de la proposition de créer un art. 111*k* LEI, le Conseil fédéral constate que les exigences correspondent aux art. 51, par. 2 et 4, et 37, par. 5, des règlements de l'UE sur l'interopérabilité. Or ces règlements s'appliquent de manière contraignante à la Suisse dès lors qu'ils ont été repris dans notre législation. L'arrêté fédéral ne reprend expressément les dispositions de règlements de l'UE dans sa propre législation que là où une telle répétition s'avère nécessaire, notamment en vertu de la LPD. Doivent par exemple y être formellement réglementés les finalités du traitement de données, les droits d'accès, le transfert de données et les sanctions prévues en cas de traitement abusif des données. Toutefois, une répétition, en droit suisse, de tous les articles figurant dans les règlements de l'UE sur l'interopérabilité ne serait pas pertinente.

S'agissant des demandes ayant trait aux autorités de surveillance, les règlements de l'UE sur l'interopérabilité renvoient à la directive (EU) 2016/680 et au règlement (EU) 2016/679. Dans les domaines où il est renvoyé à la directive (EU) 2016/680, l'autorité de surveillance a été dotée des compétences prévues dans ladite directive (cf. art. 21 à 25 LPDS).

En ce qui concerne les mécanismes de contrôle, il faut souligner que la Suisse dispose déjà de structures éprouvées et que celles-ci ont été continuellement développées dans le domaine des systèmes d'information Schengen-Dublin. Le PFPDT et les autorités cantonales de protection des données collaborent activement, dans le

15 RS **235.1**

16 Cf. message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF **2017** 6565

cadre de leurs compétences respectives, et veillent à exercer une surveillance coordonnée du traitement des données à caractère personnel. Le PFPDT coordonne les tâches de surveillance avec les autorités cantonales de protection des données; il est le point de contact national du CEPD. Le PFPDT a été consulté au sujet des tâches qui lui incombent dans le cadre de ce projet et n'y a pas formulé d'objection. Les dispositions relatives au respect des droits des personnes concernées (droits d'accès, de rectification et d'effacement), à la sécurité des données et au contrôle de leur traitement seront édictées dans l'ordonnance d'exécution.

Enfin, conformément aux règlements de l'UE sur l'interopérabilité, les États Schengen/Dublin doivent veiller à ce que le droit national punisse tout traitement ou échange de données illicite. La disposition pénale correspondante figure déjà dans le projet, à l'art. 120*d* P-LEI. L'article 120*d* (droit en vigueur) a été créé en application du règlement VIS de l'UE[17]. Il a par la suite été complétée par l'EES et par ETIAS (FF **2019** 4397 et **2020** 2779 ; cf. ch. 4.1). Le présent projet y ajoute encore le MID et le CIR. Aucune raison justifiant d'ajuster le niveau de répression pénale n'a été identifiée.

Stigmatisation et discrimination à l'encontre des ressortissants d'États tiers

Plusieurs participants à la consultation (AsyLex, USS, OSAR, PS) considèrent ce projet comme un nouveau pas vers la discrimination, l'inégalité de traitement et la stigmatisation des ressortissants d'États tiers par rapport aux citoyens de l'UE/AELE. Ils estiment que le recours systématique aux données biométriques illustre de manière patente ce phénomène. Ils critiquent aussi la tendance sous-jacente à considérer principalement la migration sous l'angle de la sécurité intérieure.

Le Conseil fédéral prend acte de ces préoccupations. Il fait cependant remarquer que l'interopérabilité n'entraîne pas de collecte de données supplémentaires. Elle ne constitue donc nullement une discrimination à l'encontre des ressortissants d'États tiers. Au contraire, le recours aux données biométriques facilitera l'identification sûre des personnes et, par là même, la mobilité des ressortissants d'États tiers voyageant dans l'espace Schengen en toute légalité.

Information de l'État ayant émis le signalement pour les recherches Interpol

Certains participants à la consultation (AsyLex, USS, OSAR) ont critiqué le fait que l'autorité ayant émis un signalement dans les bases de données d'Interpol (donc, potentiellement aussi un État tiers) soit informée de l'heure et du lieu de la recherche lors d'un résultat positif obtenu après consultation des bases de données d'Interpol via l'ESP. Ils estiment, en effet, que cette information pourrait conduire à des abus.

17 Règlement (CE) n° 7672008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États Schengen sur les visas de court séjour (règlement VIS), JO L 218 du 13.8.2008, p. 60, modifié en dernier lieu par le règlement (UE) 2019/817, JO L 135 du 22.5.2019, p. 27.

À cet égard, le Conseil fédéral relève que, conformément aux prescriptions de l'UE sur l'interopérabilité, les résultats positifs ne sont pas communiqués à l'État ayant émis le signalement. L'UE et Interpol sont par ailleurs en train de mener des discussions sur l'extension de l'interopérabilité aux bases de données d'Interpol afin que cette condition puisse être respectée.

Constitutionnalité

Le PS critique le manque de base constitutionnelle matérielle, estimant que la mise en œuvre de l'interopérabilité va au-delà de la politique extérieure puisqu'elle empiète sur les domaines de l'asile, de la migration et de la sécurité.

Le Conseil fédéral relève que la mise en œuvre de l'interopérabilité dispose d'une base constitutionnelle (art. 54, al. 1, de la Constitution [Cst.][18]), puisque l'interopérabilité concerne l'espace Schengen, auquel la Suisse est associée, et relève donc de la politique extérieure. Si cette coopération comprend aussi des aspects liés à la sécurité et à la migration, c'est bien cette disposition de la Cst. qui est déterminante s'agissant de la reprise de traités internationaux.

Le Conseil fédéral reconnaît que l'interopérabilité a des répercussions de grande ampleur, puisqu'elle concerne tous les ressortissants d'États tiers et touche plusieurs droits fondamentaux, dont le droit à la liberté de mouvement (art. 10, al. 2, Cst.). Il considère cependant que l'interopérabilité ne limite pas ce dernier de manière excessive. Un autre droit fondamental est celui d'être protégé contre l'emploi abusif de données à caractère personnel (art. 13, al. 2, Cst.). Le Conseil fédéral souligne ici le rôle en matière de surveillance du PFPDT et des autorités cantonales de protection des données. Il fait également observer que l'interopérabilité ne concerne pas directement le domaine de l'asile. Enfin, elle n'a aucune incidence sur les conditions d'entrée et de séjour.

La Suisse s'engage en tout état de cause à plusieurs niveaux en faveur des personnes nécessitant une protection. C'est ainsi que le Conseil fédéral a adopté en 2019 un programme de réinstallation dans le cadre duquel il fixe, par périodes successives de 2 ans, les conditions d'accueil de réfugiés particulièrement vulnérables. La Suisse peut également octroyer des visas humanitaires dans les cas où il y a tout lieu d'estimer que la vie ou l'intégrité physique d'une personne sont directement, sérieusement et concrètement menacées dans son pays d'origine ou de provenance (art. 4, al. 2, de l'ordonnance du 15 août 2018 sur l'entrée et l'octroi de visas[19]).

4 Principes généraux des règlements de l'UE

4.1 Vue d'ensemble

L'interopérabilité est réglée dans deux règlements différents au niveau de l'UE étant donné que les dispositions s'adressent à des États dont le degré de participation à la coopération Schengen varie. Le règlement IOP Frontières concerne le domaine des

18 RS **101**
19 RS **142.204**

frontières et des visas, tandis que le règlement IOP Police concerne le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration. Ces deux règlements de l'UE se recouvrent à quelques exceptions près. L'interopérabilité n'a pas pour but de créer des banques de données supplémentaires, mais d'intégrer de nouvelles fonctions dans des systèmes d'information existants et futurs.

Les deux règlements de l'UE sur l'interopérabilité ont servi de cadre à la création de quatre nouveaux composants centraux pour les systèmes d'information de l'UE:

- l'ESP permettra aux autorités compétentes de consulter simultanément, en une seule requête, plusieurs systèmes d'information de l'UE;
- le sBMS permettra de consulter simultanément plusieurs systèmes d'information de l'UE à l'aide de données biométriques;
- le CIR contiendra les données d'identité (par ex. nom et date de naissance), les données des documents de voyage et les données biométriques de ressortissants d'États tiers et facilitera ainsi leur identification;
- le MID détectera des liens entre des données existantes et nouvelles dans différents systèmes d'information de l'UE et contribuera ainsi à la lutte contre la fraude à l'identité.

Les systèmes d'information et banques de données de l'UE suivants sont concernés par les règlements de l'UE sur l'interopérabilité:

- le Système d'information Schengen (SIS), qui contient des informations sur des personnes disparues ou recherchées et les véhicules et objets recherchés et dans lequel sont signalés les interdictions d'entrée et désormais aussi les des décisions de renvoi;
- le système d'information sur les visas (VIS), qui contient les informations sur les visas Schengen;
- Eurodac, la base de données contenant les empreintes digitales de requérants d'asile et de personnes appréhendées lors de leur entrée irrégulière dans l'espace Schengen;
- le système européen d'information sur les casiers judiciaires de ressortissants d'États tiers (ECRIS-TCN), un système électronique permettant l'échange d'informations provenant d'extraits de casiers judiciaires entre les États de l'UE;
- le système d'entrée et de sortie (EES), dans lequel figureront désormais les données liées à l'entrée et à la sortie des ressortissants d'États tiers qui entrent dans l'espace Schengen pour un séjour d'une durée n'excédant pas 90 jours par période de 180 jours, de même que les interdictions d'entrée;
- le système européen d'information et d'autorisation concernant les voyages (ETIAS), par lequel les ressortissants d'États tiers exemptés de visa devront demander et obtenir une autorisation de voyage avant d'entrer dans l'espace Schengen;
- les données d'Europol (*Europol Information System*);
- la base de données d'Interpol sur les documents de voyage volés ou perdus (*Stolen and Lost Travel Documents*, SLTD) et celle sur les documents de voyage associés aux notices (*Travel Documents Associated with Notices*, TDAWN).

La Suisse participe déjà aux systèmes d'information SIS, VIS et Eurodac. Une participation aux nouveaux systèmes EES et ETIAS, qui font aussi partie de l'acquis de Schengen, est également prévue. La reprise et la mise en œuvre du règlement EES ont été approuvées par le Parlement en juin 2019[20]. Le message concernant la reprise et la mise en œuvre du règlement ETIAS a été adopté par le Conseil fédéral le 6 mars 2020[21] et est actuellement en discussion au Parlement. La Suisse est également tenue de reprendre, d'ici novembre 2020, les développements concernant le SIS, qui créent des possibilités supplémentaires pour la coopération en matière de police et de migration, notamment par l'introduction d'un nouveau signalement de retour. Le Conseil fédéral a adopté le message relatif aux règlements SIS le 6 mars 2020[22]. Ce projet est actuellement en discussion au Parlement.

Le système ECRIS-TCN ne constitue en revanche pas un développement de l'acquis de Schengen et la Suisse n'y a donc pas accès. Elle examine actuellement la possibilité d'y participer. C'est pourquoi il est question de l'interopérabilité des « systèmes d'information de l'UE » dans les règlements de l'UE. Cette formulation est également utilisée dans le présent message, à l'exception du chapitre 7. S'agissant de la mise en œuvre au niveau juridique en Suisse, on utilise en revanche la formulation « systèmes d'information Schengen-Dublin », étant donné que seuls ces derniers doivent être repris dans le droit suisse.

Actuellement, la Suisse ne dispose pas non plus d'un accès direct aux données d'Europol. En vertu des art. 8 et 9 de l'accord du 24 septembre 2004 entre la Confédération suisse et l'Office européen de police[23], la Suisse peut adresser des demandes à Europol afin d'obtenir des informations issues du système d'information d'Europol. La Suisse s'efforce d'obtenir un accès direct aux données Europol. Des discussions sont en cours afin de déterminer si l'UE fournira aux États associés à Schengen un accès direct à ses données via l'ESP. Des vérifications sont en cours afin d'établir comment les composants centraux pourront accéder aux données d'Europol. Le droit de consultation devra toutefois s'inscrire dans le cadre légal actuel (accord de coopération entre la Suisse et Europol). Il semble donc indiqué de prévoir déjà la possibilité de l'accès via l'ESP aux données d'Europol dans la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[24] et la loi du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[25]. En tant qu'État membre, la Suisse possède un droit d'accès aux bases de données d'Interpol mentionnées plus haut.

20 FF **2019** 4397
21 FF **2020** 2779
22 FF **2020** 3361
23 RS **0.362.2**
24 RS **142.20**
25 RS **361**

4.2 Applicabilité échelonnée des règlements sur l'interopérabilité

Les deux règlements sur l'interopérabilité sont entrés en vigueur dans l'UE le 11 juin 2019, mais la grande majorité des dispositions ne deviendra applicable que plus tard. Il appartient donc à la Commission européenne de décider de la mise en service échelonnée des différents composants centraux, et les dispositions pertinentes ne seront applicables qu'à partir des dates fixées (cf. art. 79 du règlement IOP Frontières et art. 75 du règlement IOP Police). Les conditions pour la mise en service des différents composants centraux incluent notamment le fait d'achever avec succès un test complet du composant central concerné en collaboration avec les États Schengen et les agences européennes. En outre, les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données doivent être en place (art. 72 du règlement IOP Frontières, art. 68 du règlement IOP Police). Les différents composants centraux seront donc opérationnels à des moments différents. Selon le calendrier actuel de la Commission européenne, le sBMS sera mis en service d'ici la fin 2021, le CIR d'ici l'été 2022, l'ESP d'ici l'été 2023 et le MID d'ici la fin 2023. Différentes phases de transition sont par ailleurs prévues avant que chaque composant central puisse être mis en service.

Enfin, l'art. 79 du règlement IOP Frontières et l'art. 75 du règlement IOP Police précisent qu'en ce qui concerne Eurodac, ces deux règlements s'appliquent à partir de la date d'application de la refonte du règlement (UE) 603/2013[26]. Le raccordement d'Eurodac au cadre de l'interopérabilité est néanmoins bien prévu, raison pour laquelle Eurodac est mentionné au ch. 3. On ne dispose cependant pas encore de dispositions concrètes en la matière. C'est pourquoi la mise en œuvre légale en Suisse n'aura lieu qu'au moment de la reprise du règlement Eurodac révisé.

5 Contenu des règlements de l'UE

Ce chapitre fournit une vue d'ensemble du contenu des deux règlements européens, en mettant l'accent sur les quatre composants centraux (ch. 5.1). D'autres nouveautés qui ont également des effets sur la Suisse sont exposées au ch. 5.2. Il s'agit par exemple de dispositions concernant l'obligation d'information, les exigences en matière de qualité des données et les modifications apportées à d'autres actes juridiques.

26 Règlement (UE) n ° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 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 180 du 29.6.2013, p. 1.

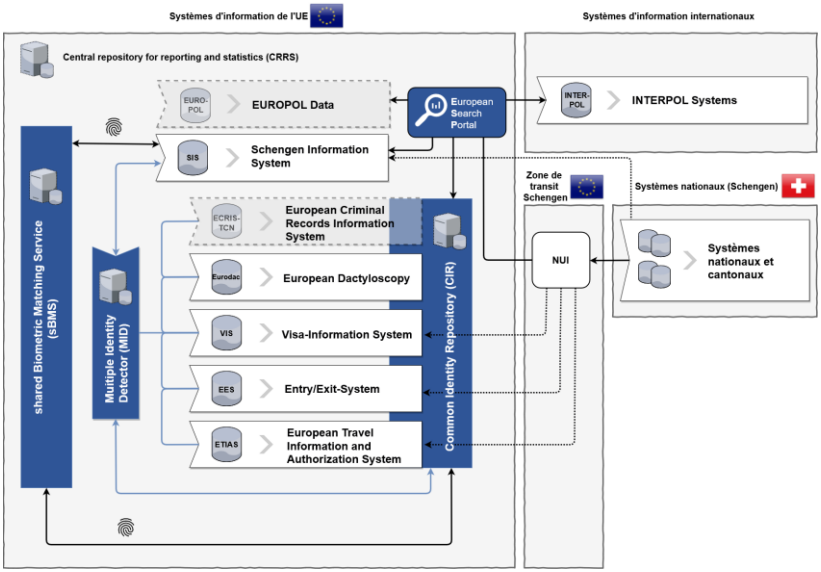
Étant donné que les deux règlements se recouvrent à quelques exceptions près, leur contenu est présenté comme s'ils formaient un seul texte. Les numéros de chapitres et d'articles sont pour la plupart les mêmes. Ce n'est que vers la fin du chapitre VIII des règlements de l'UE que les numéros d'articles commencent à diverger: les références à ces articles sont donc indiquées séparément.

5.1 Les quatre nouveaux composants centraux

Les quatre nouveaux composants centraux forment le noyau de l'interopérabilité. Grâce à eux, les différents systèmes d'information de l'UE pourront communiquer entre eux de façon ciblée. L'échange d'informations deviendra plus efficace et les lacunes en matière de sécurité seront comblées. Les différents composants centraux se soutiennent et se complètent mutuellement. Ce n'est qu'en les combinant qu'il sera possible d'atteindre les objectifs de l'interopérabilité dans leur totalité.

L'ESP permettra à l'avenir d'effectuer simultanément des recherches dans plusieurs systèmes d'information de l'UE. Via l'ESP, il sera possible aussi bien de consulter directement les données dans les différents systèmes (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN, bases de données d'Europol et d'Interpol, cf. ch. 4.1) que d'accéder aux données dans le CIR. Le MID permettra de mettre au jour des cas d'identités multiples entre les différents systèmes, en comparant les données du CIR avec celles du SIS. Pour la comparaison des données biométriques, le MID aura recours au sBMS, tandis que la comparaison avec les données d'identité et les données issues de documents de voyage sera réalisée via l'ESP. Ensemble, les quatre composants centraux permettent non seulement d'échanger plus facilement des informations et d'identifier correctement des personnes, mais aussi de détecter des cas d'identités multiples et de fraude à l'identité.

Le schéma ci-dessous montre comment les composants centraux sont reliés entre eux et quels systèmes ils concernent. La NUI (*National Uniform Interface*) est l'interface qui établit une connexion standardisée entre les systèmes nationaux des États Schengen et les composants centraux de l'UE. Pour ETIAS, l'EES et le VIS, une connexion sera également établie via la NUI entre le composant de l'UE concerné et les composants nationaux. Les sous-chapitres suivants présentent en détail chaque composant central de l'interopérabilité.



5.1.1 Portail de recherche européen (ESP) (chap. II)

La création du portail de recherche européen (ESP) est un élément central de l'interopérabilité. L'ESP permettra aux autorités compétentes, en fonction de leurs droits d'accès, d'accéder rapidement, efficacement, systématiquement, sans interruptions et de façon contrôlée aux différents systèmes d'information de l'UE et aux bases de données d'Europol et d'Interpol (art. 6). Grâce à l'ESP, les autorités compétentes pourront accéder en une seule requête à toutes les informations pertinentes pour elles et se faire une image complète de la personne contrôlée.

Utilisation du portail de recherche européen (art. 7)

Toutes les autorités nationales et agences européennes autorisées à accéder à au moins un des systèmes d'information de l'UE (EES, ETIAS, VIS, SIS, Eurodac, bases de données d'Europol ou ECRIS-TCN), au CIR, au MID ou aux bases de données d'Interpol seront habilitées à consulter l'ESP. Les autorités compétentes des États Schengen et les services de l'UE utiliseront l'ESP pour mener des recherches dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN ainsi que pour les recherches dans le CIR pour les motifs visés aux art. 20 à 22 (pour des informations détaillées sur les recherches dans le CIR, cf. ch. 5.1.3). Elles pourront également utiliser l'ESP pour mener des recherches dans le SIS central ainsi que dans les bases de données d'Europol et d'Interpol. Les droits d'accès des autorités concernées à chacun des systèmes restent identiques.

Profils des utilisateurs du portail de recherche européen (art. 8)

L'agence eu-LISA créera, en collaboration avec les États Schengen, un profil pour chaque catégorie d'utilisateurs de l'ESP. Chaque profil contiendra notamment des informations indiquant quels systèmes d'information de l'UE et bases de données d'Europol et d'Interpol peuvent être interrogés par l'utilisateur en question. Ce sont les bases juridiques régissant chacun de ces systèmes qui détermineront quelles autorités peuvent avoir accès aux systèmes d'information concernés et dans quels buts. Les profils des utilisateurs seront réexaminés au moins une fois par an par l'eu-LISA en collaboration avec les États Schengen et, si nécessaire, mis à jour.

Requêtes (art. 9)

Une requête pourra être effectuée via l'ESP sur la base de données d'identité, de données des documents de voyage ou de données biométriques. L'ESP interrogera simultanément tous les systèmes d'information pertinents (EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN et CIR ainsi que les bases de données d'Europol et d'Interpol), conformément au profil d'utilisateur. Pour autant que des données soient disponibles dans l'un de ces systèmes, elles s'afficheront pour l'utilisateur via l'ESP dans la limite de ses droits d'accès. L'utilisateur verra également de quel système d'information de l'UE proviennent les données, sauf s'il s'agit d'une requête du CIR pour identification en vertu de l'art. 20. Dans ce cas, l'objectif est simplement d'identifier une personne, mais les autorités de police compétentes ne doivent pas apprendre dans quel système les données la concernant sont enregistrées (cf. ch. 5.1.3 relatif à l'art. 20). Lors de consultations du CIR en vertu de l'art. 22 à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, les autorités de poursuite pénale pourront uniquement voir si des données concernant une personne figurent dans un système d'information. Les données à proprement parler ne seront cependant pas affichées. L'accès aux données concernées devra être demandé séparément (cf. ch. 5.1.3 relatif à l'art. 22). Lors de requêtes dans les bases de données d'Interpol via l'ESP, l'État ayant émis le signalement n'est pas informé.

Tenue de registres (art. 10)

L'eu-LISA et les États Schengen devront tenir des registres de toutes les requêtes faites via l'ESP. Les États Schengen tiendront des registres de l'utilisation de l'ESP jusqu'à l'échelon des collaborateurs. Les registres ne pourront être utilisés que pour contrôler la protection des données. Ils devront être protégés des accès non autorisés et effacés un an après leur création, à moins qu'ils soient nécessaires à des procédures de contrôle qui ont déjà été engagées.

Procédures de secours en cas d'impossibilité technique d'utiliser le portail de recherche européen (art. 11)

L'art. 11 règle la procédure à suivre au cas où l'ESP ne pourrait pas être utilisé pour des raisons techniques. Si c'est le cas, l'eu-LISA le notifiera de manière automatisée aux utilisateurs de l'ESP. En cas de défaillance de l'infrastructure nationale d'un

État Schengen, ce dernier le notifiera de manière automatisée à l'eu-LISA et à la Commission européenne. Jusqu'à ce qu'il soit remédié à la défaillance technique, les États membres pourront consulter directement les systèmes d'information de l'UE ou le CIR.

Période transitoire pour l'utilisation du portail de recherche européen

L'art. 67 du règlement IOP Frontières et l'art. 63 du règlement IOP Police précisent que l'utilisation de l'ESP est facultative pendant les deux premières années à compter de la mise en service du composant central. Ce délai peut être prolongé une seule fois et d'une année au maximum.

5.1.2 Service partagé d'établissement de correspondances biométriques (sBMS) (chap. III)

Le Service partagé d'établissement de correspondances biométriques (sBMS) permettra d'effectuer des recherches simultanées dans plusieurs systèmes d'information de l'UE à l'aide de données biométriques (art. 12). Les règlements de l'UE utilisent l'abréviation « BMS », qui est déjà en usage dans un autre contexte dans la législation suisse. Afin d'éviter les confusions, on utilisera donc ici l'abréviation « sBMS ».

Stockage de modèles biométriques dans le service partagé d'établissement de correspondances biométriques (art. 13)

Le sBMS stockera les modèles biométriques qu'il génère à partir des données biométriques de l'EES, du VIS, du SIS, de l'ECRIS-TCN et, par la suite, d'Eurodac. Les modèles biométriques sont une représentation mathématique obtenue par l'extraction de caractéristiques des données biométriques et se limitant aux caractéristiques nécessaires pour procéder à des identifications et à des vérifications (art. 4, par. 12). ETIAS n'est pas concerné, puisqu'il ne contient pas de données biométriques. Chaque modèle contiendra une référence au système d'information de l'UE d'où il provient et une référence aux enregistrements concrets qui y figurent. Seuls les modèles biométriques respectant une norme minimale de qualité pourront être ajoutés au sBMS.

Recherche dans des données biométriques à l'aide du service partagé d'établissement de correspondances biométriques (art. 14)

La recherche de données biométriques dans le CIR et le SIS se fera par le biais des modèles biométriques contenus dans le sBMS et ne sera autorisée que conformément aux finalités prévues.

Conservation des données dans le service partagé d'établissement de correspondances biométriques (art. 15)

Les modèles biométriques et les renvois aux systèmes d'information de l'UE dont ils sont issus ne seront stockés dans le sBMS qu'aussi longtemps que les données

biométriques du CIR (tirées du VIS, de l'EES, d'ETIAS, d'Eurodac et de l'ECRIS-TCN) ou du SIS seront disponibles. Ils seront ensuite effacés de manière automatisée.

Tenue de registres (art. 16)

L'eu-LISA et les États Schengen auront l'obligation de tenir des registres de toutes les opérations de traitement de données. Les dispositions concernant l'utilisation des registres et les mesures de sécurité à prendre qui sont décrites au ch. 5.1.1 au sujet de l'art. 10 s'appliquent par analogie.

5.1.3 Répertoire commun de données d'identité (CIR) (chap. IV)

Un dossier individuel sera créé dans le CIR pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN. Le CIR constituera ainsi une partie de ces systèmes. Les données resteront enregistrées dans le système correspondant. L'objectif est de faciliter l'identification des personnes qui sont enregistrées dans l'un de ces systèmes d'information. Le CIR permettra notamment de simplifier et d'améliorer l'accès des autorités de poursuite pénale aux systèmes d'information de l'UE non consacrés à la poursuite pénale à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'enquêtes en la matière (art. 17 en relation avec l'art. 22). En raison de l'architecture technique complexe du SIS, ses données ne feront pas partie du CIR.

Données du répertoire commun de données d'identité (art. 18)

Le CIR enregistrera les données d'identité ainsi que, si elles sont disponibles, les données des documents de voyage et les données biométriques issues de l'EES, du VIS, d'ETIAS, de l'ECRIS-TCN et d'Eurodac. Il stockera les données séparément en fonction du système d'information d'où elles proviennent (séparation logique). Pour chaque bloc de données enregistré (« enregistrement concret » selon la terminologie de l'UE), le CIR comportera une référence au système d'information de l'UE auquel appartiennent les données. Les droits d'accès des autorités au CIR dépendent des bases juridiques qui régissent chaque système d'information de l'UE et des droits d'accès prévus dans les règlements sur l'interopérabilité pour les fins visées aux art. 20 à 22.

Ajout, modification et suppression de données dans le répertoire commun de données d'identité (art. 19)

Les données enregistrées dans le CIR seront adaptées automatiquement dès que des données seront ajoutées, modifiées ou supprimées dans l'EES, le VIS, ETIAS, l'ECRIS-TCN et, par la suite, dans Eurodac. Lorsqu'un lien blanc ou rouge sera créé dans le MID concernant des données du CIR (cf. ch. 5.1.4), au lieu de créer un nouveau dossier individuel, le CIR ajoutera les nouvelles données au dossier individuel des données liées.

Accès au répertoire commun de données d'identité pour identification (art. 20)

Le CIR vise à faciliter l'identification de ressortissants d'États tiers. C'est pourquoi l'art. 20 prévoit que les agents de police, lors des contrôles à l'intérieur d'un pays, peuvent, à des fins d'identification, consulter le CIR à certaines conditions par le biais de l'ESP. Le par. 1 établit la liste des cas dans lesquels une telle consultation du CIR est possible: a) lorsqu'un service de police n'est pas en mesure d'identifier une personne en raison de l'absence d'un document de voyage ou d'un autre document crédible prouvant son identité ; b) lorsqu'un doute subsiste quant aux données d'identité fournies par une personne ; c) lorsqu'un doute subsiste quant à l'authenticité du document de voyage ou d'un autre document crédible ; d) lorsqu'un doute subsiste quant à l'identité du titulaire d'un document de voyage ou d'un autre document crédible, ou e) lorsqu'une personne n'est pas en mesure de coopérer lors d'une identification ou refuse de le faire. Une interrogation du CIR pour identification ne peut viser un mineur de moins de 12 ans, à moins que ce ne soit dans l'intérêt supérieur de l'enfant.

Normalement, l'interrogation du CIR se fera à l'aide des données biométriques de la personne relevées directement lors d'un contrôle d'identité (par. 2). Si les données biométriques de la personne ne peuvent pas être utilisées ou si la requête introduite avec ces données échoue, la requête sera introduite à l'aide des données d'identité de cette personne, combinées aux données du document de voyage. Si des données figurent dans le CIR au sujet de la personne en question, l'autorité de police sera habilitée à les consulter, mais sans que le système affiche de quel système d'information de l'UE elles proviennent. Le par. 4 prévoit que les données du CIR peuvent être utilisées pour identifier les victimes d'attentats, d'accidents ou de catastrophes naturelles ou les restes humains non identifiés. Les États Schengen qui souhaitent faire usage de ces deux nouvelles possibilités doivent adapter leurs lois nationales en conséquence et désigner les autorités qui seront habilitées à effectuer la requête.

Accès au répertoire commun de données d'identité pour la détection d'identités multiples (art. 21)

L'accès au CIR est également prévu en relation avec les liens MID (cf. ch. 5.1.4). Les autorités compétentes seront autorisées à accéder aux données reliées entre elles dans le CIR pour la vérification des différentes identités en cas de lien jaune et pour la lutte contre la fraude à l'identité en cas de lien rouge.

Interrogation du répertoire commun de données d'identité à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière (art. 22)

Les autorités chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, désignées par chaque pays en fonction des bases juridiques des différents systèmes (ci-après « autorités désignées ») ne disposent pas d'office d'un accès direct aux données de l'EES, du VIS, d'ETIAS ou d'Eurodac, mais doivent le demander auprès d'un point d'accès central, également défini dans le droit national.

Avec l'interopérabilité, l'accès des autorités désignées aux données figurant dans ces systèmes doit être soumis à de nouvelles règles. Concrètement, une procédure en deux étapes passant par une consultation du CIR est prévue. Dans la mesure où des motifs suffisants justifient une consultation des systèmes d'information de l'UE aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, en particulier lorsqu'il y a lieu de suspecter que la personne en question est enregistrée dans l'un de ces systèmes, les autorités désignées et Europol pourront consulter le CIR. Cette première étape se fera selon le mécanisme dit « hit / no hit » (réponse positive / pas de réponse positive). En cas de réponse positive (à savoir si des données concernant une personne figurent dans l'EES, ETIAS, le VIS ou Eurodac), le CIR signalera à l'autorité requérante dans quel système d'information de l'UE les données figurent. Celle-ci aura ensuite la possibilité, comme aujourd'hui, de rédiger une demande d'accès complet à au moins un des systèmes d'information de l'UE ayant donné une réponse positive. L'autorisation d'accès complet aux données concernées issues de l'EES, d'ETIAS, du VIS ou d'Eurodac restera soumise aux conditions et procédures fixées dans les bases légales des systèmes d'information sous-jacents. Si, à titre exceptionnel, l'autorité ne demande pas un accès complet, elle doit dûment le justifier par écrit et cette justification doit être consignée.

Conservation des données dans le répertoire commun de données d'identité (art. 23)

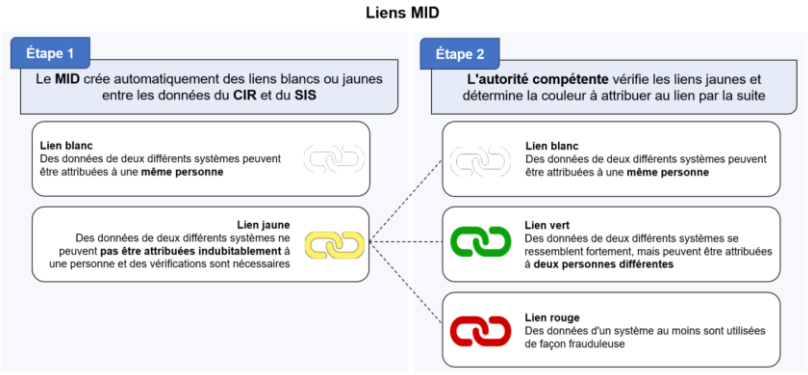
Les données seront supprimées du CIR de manière automatisée conformément aux dispositions relatives à la conservation des données du système d'information de l'UE dont elles sont issues. Le dossier individuel ne sera stocké dans le CIR qu'aussi longtemps que les données correspondantes le seront dans au moins un des systèmes d'information de l'UE.

Tenue de registres (art. 24)

L'eu-LISA tiendra des registres de toutes les opérations de traitement de données et requêtes dans le CIR. Les États Schengen auront l'obligation de tenir des registres sur les requêtes effectuées conformément aux art. 20 à 22, et Europol sur les accès fondés sur les art. 21 et 22. Les dispositions concernant l'utilisation des registres et les mesures de sécurité à prendre qui sont décrites au ch. 5.1.1 au sujet de l'art. 10 s'appliquent par analogie.

5.1.4 Détecteur d'identités multiples (MID) (chap. V)

Le MID est le quatrième composant central. Il doit contribuer à identifier des personnes qui utilisent plusieurs identités ou de fausses identités. L'objectif du MID est double: faciliter les contrôles d'identité et lutter contre la fraude à l'identité. À cette fin, il créera et stockera des dossiers de confirmation d'identité contenant des liens entre les données des systèmes d'information de l'UE (art. 25). Concrètement, le MID examinera si les données personnelles, données des documents de voyage ou les données biométriques nouvellement saisies dans un système existent déjà dans d'autres systèmes. Suivant la combinaison, le MID établira automatiquement des liens dits « blancs » ou « jaunes ». Tous les liens jaunes devront être vérifiés manuellement par les autorités compétentes: ces dernières contrôleront les différentes identités et, selon qu'il s'agit de la même personne ou d'une autre personne, le lien sera classé comme rouge, vert ou blanc. Le schéma ci-dessous fournit une première vue d'ensemble de ces processus. La procédure exacte et la signification des liens sont expliquées plus en détail ci-après et illustrées par trois exemples à la fin du chapitre.



Accès au détecteur d'identités multiples (art. 26)

L'art. 26 règle qui peut accéder aux données enregistrées dans le MID et à quelles fins. D'une part, les autorités compétentes seront autorisées à y accéder aux fins de la vérification manuelle de différentes identités conformément à l'art. 29, à savoir les autorités qui saisissent ou mettent à jour des données dans l'EES, le VIS, ETIAS, l'ECRIS-TCN, le SIS et Eurodac. Ces autorités sont désignées dans les bases juridiques des différents systèmes d'information. D'autre part, les autorités des États Schengen et les agences de l'UE (en l'occurrence, Europol et le Corps européen de garde-frontières et de garde-côtes) auront accès, via le MID, aux liens rouges s'ils ont accès à au moins un système d'information de l'UE concerné. L'accès aux liens blancs ou verts sera possible si les autorités ont accès aux deux systèmes d'information de l'UE dont sont issues les données formant le lien en question.

Détection d'identités multiples (art. 27)

L'art. 27 décrit comment se déroule la détection d'identités multiples. Un tel processus sera déclenché lors de chaque saisie ou mise à jour de données dans l'un des systèmes d'information de l'UE (VIS, SIS, ETIAS, EES). Pour ce faire, les nouvelles données seront comparées avec celles figurant déjà dans le CIR et le SIS. Le sBMS se chargera de la comparaison des données biométriques et l'ESP de celle des données d'identité et des données des documents de voyage. Une détection d'identités multiples ne sera lancée que pour comparer des données entre les différents systèmes d'information de l'UE.

Résultats de la détection d'identités multiples (art. 28)

Les résultats possibles d'une détection d'identités multiples et les procédures qui en découlent sont décrits à l'art. 28. Lorsque la recherche ne génère aucune correspondance avec des données d'autres systèmes d'information de l'UE, la saisie de données a lieu conformément aux bases juridiques applicables. Lorsque la recherche génère une ou plusieurs correspondances, des liens sont créés entre les données (nouvelles ou mises à jour) utilisées pour lancer la recherche et celles figurant déjà dans un autre système d'information de l'UE. Lorsque plusieurs correspondances sont générées, un lien est créé entre toutes les données concernées. Si ces données sont déjà liées, le lien existant est étendu aux nouvelles données.

Lorsque les données d'identité dans les dossiers liés sont identiques ou similaires, un lien blanc est créé automatiquement. Par contre, lorsque les données d'identité ne peuvent pas être considérées comme similaires, un lien jaune est créé et une vérification manuelle de la part des autorités compétentes s'impose. Les critères déterminant à partir de quel moment des données d'identité sont considérées comme identiques ou similaires sont définis par la Commission européenne et fixés dans un acte délégué que la Suisse est tenue de reprendre en tant que développement de l'acquis de Schengen. Tous les liens sont enregistrés dans un dossier de confirmation d'identité conformément à l'art. 34.

Vérification manuelle des différentes identités et autorités responsables (art. 29)

Si un lien jaune est créé lors de la détection d'identités multiples par le MID, les différentes identités doivent faire l'objet d'une vérification manuelle. L'autorité responsable de cette vérification est celle qui crée ou met à jour les données dans l'un des systèmes d'information de l'UE.

Le par. 2 prévoit une exception à cette règle générale. La vérification manuelle d'un lien avec un signalement du SIS conformément aux art. 26, 32, 34 ou 36 du règlement (UE) 2018/1862[27] incombe ainsi au bureau SIRENE de l'État Schengen qui a créé le signalement. Les catégories de signalements suivantes sont concernées: signalement en vue d'une arrestation aux fins d'extradition (art. 26); personnes disparues (art. 32); communication du lieu de séjour (art. 34); contrôles discrets, contrôles d'investigation ou contrôles spécifiques (art. 36). Le bureau SIRENE est donc responsable de toutes les recherches de personnes, à l'exception des interdictions d'entrée et des décisions de retour. Le MID indique l'autorité responsable dans le dossier de confirmation d'identité.

La vérification doit avoir lieu sans délai. Dès qu'elle est achevée, l'autorité responsable met à jour le lien en le classant comme lien vert, rouge ou blanc conformément aux art. 31 à 33. Le lien est alors considéré comme vérifié. L'art. 29, par. 4, du règlement IOP Frontières contient des dispositions supplémentaires concernant la vérification qui doit être menée lors de la création ou de la mise à jour de dossiers dans l'EES. La vérification doit être lancée en présence de la personne concernée et cette dernière doit avoir la possibilité de s'exprimer sur la situation. Si la vérification manuelle a lieu à une frontière extérieure de Schengen, l'ensemble du processus doit avoir lieu dans un délai de 12 heures.

En cas de création de plusieurs liens, chacun d'entre eux doit être vérifié. Lorsqu'elles envisagent la création d'un nouveau lien, les autorités responsables doivent tenir compte des liens existants entre les données ayant généré une correspondance.

Lien jaune (art. 30)

Un lien est classé comme jaune lorsque la détection d'identités multiples aboutit à des résultats peu clairs qui n'ont pas encore été vérifiés manuellement. C'est notamment le cas lorsque les données liées comportent les mêmes données d'identité mais ont des données biométriques différentes, ou lorsque les données biométriques coïncident mais que les données d'identité divergent, ce qui est possible par exemple en cas de mariage entraînant un changement de nom. Lorsqu'un lien est classé comme jaune, une vérification manuelle de la part des autorités compétentes est nécessaire dans tous les cas conformément à l'art. 29.

27 Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission, JO L 312 du 7.12.2018, p. 56, modifié en dernier lieu par le règlement (UE) 2019/817, JO L 135 du 22.5.2019, p. 27

Lien vert (art. 31)

Un lien n'est classé comme vert qu'une fois que la vérification manuelle a eu lieu. Il indique que les données d'identité liées ne désignent pas la même personne. C'est notamment le cas lorsque les données liées ont des données biométriques différentes mais comportent les mêmes données d'identité parce que deux personnes se trouvent avoir le même nom et la même date de naissance. Le contrôle d'identité des personnes concernées voyageant légalement en est facilité par la suite.

Si une autorité d'un État Schengen dispose d'éléments suggérant qu'un lien vert a été enregistré de manière incorrecte, qu'il n'est pas à jour ou que des données ont été traitées en violation des règlements de l'UE sur l'interopérabilité, elle doit vérifier les données concernées et, si nécessaire, rectifier ou supprimer les liens. L'autorité responsable à l'origine de la vérification manuelle des différentes identités doit en être informée sans retard.

Lien rouge (art. 32)

Un lien n'est classé comme rouge qu'une fois que la vérification manuelle a eu lieu. Il indique un cas d'identités multiples illicites ou de fraude à l'identité. Différents cas de figure peuvent donner lieu à un lien rouge:

– une personne utilise plusieurs identités différentes, ce qui se manifeste par le fait que les mêmes données biométriques ou les mêmes données du document de voyage sont enregistrées sous différentes données d'identité dans différents systèmes d'information de l'UE, alors qu'elles se rapportent à une seule et même personne;

– une personne utilise le document de voyage d'une autre personne, ce qui se manifeste par le fait que les données liées comportent des données biométriques différentes alors que les données du document de voyage sont les mêmes; les données liées se rapportent donc à deux personnes différentes;

– une personne se fait passer pour une autre, ce qui se manifeste par le fait que des données biométriques différentes sont enregistrées sous les mêmes données d'identité dans différents systèmes d'information de l'UE; les données liées se rapportent donc à deux personnes différentes.

L'existence d'un lien rouge n'entraîne pas à elle seule des conséquences pour la personne en question. Des mesures ne peuvent être prises que dans le respect du droit de l'UE et du droit national. Lorsqu'un lien rouge est créé entre des données dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN, le dossier individuel stocké dans le CIR est mis à jour.

Dès qu'un lien rouge est créé, l'autorité chargée de la vérification manuelle informe, à l'aide d'un formulaire type, la personne concernée de la présence de données d'identités multiples illicites et lui indique où et comment elle peut obtenir des informations sur ces données en lui fournissant le numéro d'identification unique et l'adresse du portail en ligne (cf. ch. 5.2, Protection des données). L'autorité peut, si nécessaire, décider de ne pas informer la personne concernée afin d'assurer le res-

pect des dispositions relatives au traitement des signalements dans le SIS, de protéger la sécurité et l'ordre publics, de prévenir la criminalité ou de garantir que des enquêtes nationales ne soient pas compromises (par. 4 et 5). Chaque fois qu'un lien rouge est créé, le MID le notifie de manière automatisée aux autorités responsables des données liées.

Si une autorité d'un État Schengen dispose d'éléments suggérant qu'un lien rouge a été enregistré de manière incorrecte ou que des données ont été traitées en violation des règlements de l'UE sur l'interopérabilité, elle doit, dans la plupart des cas, vérifier les données concernées et, si nécessaire, rectifier ou effacer le lien. S'il s'agit en revanche d'un lien qui se rapporte à un signalement dans le SIS conformément aux art. 26, 32, 34 ou 36 du règlement (UE) 2018/1862, elle doit en informer immédiatement le bureau SIRENE de l'État Schengen qui a émis le signalement. Dans ce cas, le bureau SIRENE se charge de la vérification et rectifie ou efface le lien si nécessaire. L'autorité qui a reçu les informations relatives à un éventuel lien erroné informe alors immédiatement l'autorité responsable de la vérification manuelle des différentes identités de la rectification ou de l'effacement du lien rouge.

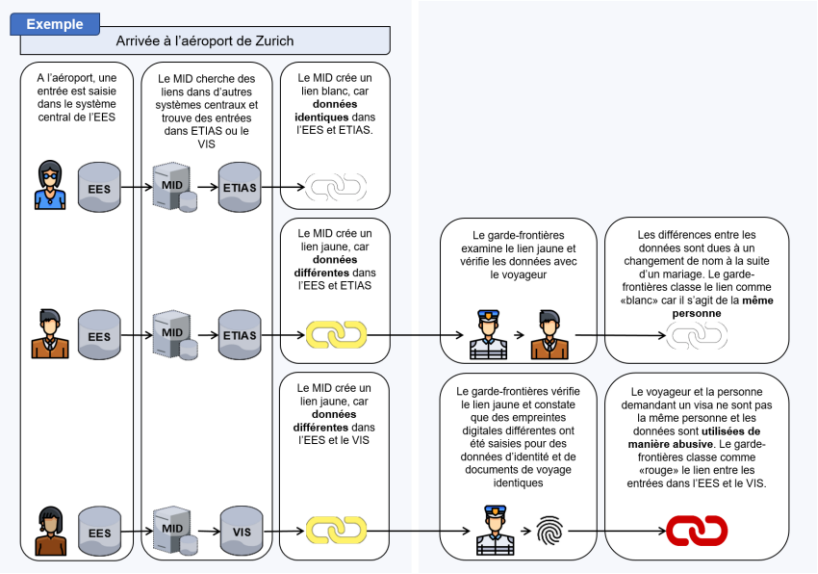
Lien blanc (art. 33)

Un lien blanc apparaît soit automatiquement lors de la détection d'identités multiples par le MID au sens de l'art. 27 (par ex. lorsque les données liées comportent les mêmes données biométriques et les mêmes données d'identité), soit comme résultat d'une vérification manuelle au sens de l'art. 29 (lorsque les données liées comportent les mêmes données biométriques mais ont des données d'identité similaires ou différentes et que l'autorité chargée de la vérification constate qu'il s'agit de la même personne). Un lien blanc indique donc que les données liées désignent une seule et même personne et, partant, que cette personne figure déjà dans au moins un autre système d'information de l'UE. La mobilité des personnes qui, par exemple, sont légalement titulaires de plusieurs documents de voyage valables sera ainsi facilitée. Lorsqu'un lien blanc est créé entre des données dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN, le dossier individuel stocké dans le CIR est mis à jour.

Lorsqu'un lien blanc est créé à la suite d'une vérification, l'autorité chargée de la vérification informe la personne concernée, à l'aide d'un formulaire type, de la présence de données d'identité similaires ou différentes et lui indique où et comment elle peut obtenir des informations concernant ces données. Comme pour les liens rouges, l'autorité peut, si nécessaire, décider de ne pas informer la personne pour des raisons de sécurité.

Si une autorité d'un État Schengen dispose d'éléments suggérant qu'un lien blanc a été enregistré de manière incorrecte, qu'il n'est pas à jour ou que des données ont été traitées en violation des règlements de l'UE sur l'interopérabilité, elle doit vérifier les données concernées et, si nécessaire, rectifier ou effacer le lien. L'autorité responsable à l'origine de la vérification manuelle des différentes identités doit être informée sans retard.

Les trois exemples ci-dessous illustrent le fonctionnement du MID et la signification des différents liens.



Les résultats de la vérification manuelle sont enregistrés dans le dossier de confirmation d'identité.

Dossier de confirmation d'identité (art. 34)

Le MID contient uniquement des dossiers de confirmation d'identité. Outre le type de lien (art. 30 à 33), le dossier indique également dans quel système d'information de l'UE sont enregistrées les données liées. Chaque dossier comprend un numéro d'identification unique permettant d'extraire les données liées des systèmes d'information de l'UE correspondants. Le dossier indique également l'autorité responsable de la vérification manuelle ainsi que la date de création ou de mise à jour du lien.

Conservation des données dans le détecteur d'identités multiples (art. 35)

Les dossiers de confirmation d'identité et leurs données, y compris les liens, ne sont stockés dans le MID qu'aussi longtemps que les données liées sont disponibles dans au moins deux systèmes d'information de l'UE. Ils sont ensuite effacés du MID de manière automatisée.

Tenue de registres (art. 36)

L'eu-LISA et les États Schengen tiendront des registres de toutes les opérations de traitement de données. Les dispositions concernant l'utilisation des registres et les mesures de sécurité à prendre qui sont décrites au ch. 5.1.1 au sujet de l'art. 10 s'appliquent par analogie.

Période transitoire pour la détection d'identités multiples

La période transitoire pour la détection d'identités multiples est réglée à l'art. 69 du règlement IOP Frontières et à l'art. 65 du règlement IOP Police. Une fois que le développement du MID sera achevé et qu'il aura été testé avec succès, toutes les données figurant dans l'EES, le VIS, Eurodac et le SIS devront être vérifiées avant la mise en service pour y détecter d'éventuelles identités multiples. Cette vérification s'effectuera exclusivement au moyen de données biométriques. L'unité centrale ETIAS en sera chargée. Si un lien jaune est établi avec un signalement du SIS conformément aux art. 26, 32, 34 ou 36 du règlement (UE) 2018/1862, le bureau SIRENE compétent sera impliqué dans la procédure de vérification. Ce n'est qu'une fois tous les liens jaunes vérifiés et mis à jour que l'unité centrale ETIAS informera la Commission européenne, qui décidera ensuite du moment de la mise en service effective du MID. Cette vérification devrait être achevée dans un délai d'un an, mais une prolongation est possible.

5.2 Autres dispositions

Outre les dispositions relatives aux quatre composants centraux, les deux règlements comprennent de nombreuses dispositions, dont le contenu est résumé ci-après. Certaines d'entre elles ne seront cependant mises en œuvre en Suisse qu'au niveau de l'ordonnance ou n'ont pas besoin d'être reprises dans le droit suisse.

Mesures soutenant l'interopérabilité (chap. VI)

Afin de rendre possible l'interopérabilité des différents systèmes d'information de l'UE, plusieurs mesures de soutien sont prévues.

L'art. 37 contient des dispositions sur les exigences en matière de qualité des données. Il prévoit d'une part des procédures automatisées pour le contrôle de qualité des données et d'autre part la mise en œuvre de normes de qualité minimales qui doivent être remplies pour stocker des données dans les systèmes d'information de l'UE et les composants centraux. Le format universel pour les messages (*Universal Message Format*, UMF) sert de nouvelle norme pour l'échange d'informations transfrontières (art. 38). Cette norme doit pouvoir être utilisée pour le développement de l'EES, d'ETIAS, de l'ESP, du CIR et du MID et pourrait également être utilisée par de futurs systèmes d'information. Un répertoire central des rapports et statistiques (*Central Repository for Reporting and Statistics*) a été mis en place à des fins d'analyse et de statistiques (art. 39). Il permettra de fournir des statistiques intersystèmes. Les données qui lui seront fournies seront rendues anonymes afin que l'identification d'individus soit impossible.

Protection des données (chap. VII)

Le chapitre VII est consacré à la protection des données. Il établit la liste des services responsables du traitement des données (art. 40) et de ceux responsables de la sécurité du traitement des données (art. 42). L'eu-LISA remplit une fonction importante dans ce domaine, puisque cette agence est responsable de la sécurité des composants centraux et de l'infrastructure de communication et qu'elle doit par exemple garantir le rétablissement en cas d'interruption.

Les États Schengen sont tenus de prendre des mesures pour vérifier que les règlements sur l'interopérabilité sont bien respectés (art. 44). L'art. 45 oblige quant à lui les États Schengen à sanctionner l'utilisation abusive de données et le traitement ou l'échange d'informations illicite. Les sanctions prévues doivent être effectives, proportionnées et dissuasives. L'art. 46 règle la question de la responsabilité en cas de dommage. En principe, toute personne ayant subi un dommage du fait d'une opération illicite de traitement de données ou de tout autre acte incompatible avec le règlement a le droit d'obtenir réparation. Le service concerné est exonéré de sa responsabilité s'il est prouvé que le fait générateur du dommage ne lui est pas imputable. Si le non-respect par un État Schengen des obligations qui lui incombent cause un dommage aux composants centraux, cet État en est tenu responsable dans la mesure où l'eu-LISA ou un autre État Schengen n'a pas pris de mesures raisonnables pour prévenir le dommage ou en atténuer les effets.

Le droit à l'information concernant des données enregistrées dans le sBMS, le CIR ou le MID est réglé à l'art. 47. Si des données à caractère personnel sont saisies pour être stockées dans le sBMS, le CIR ou le MID, la personne concernée doit en être informée en des termes clairs et simples, dans une langue qu'elle comprend.

L'art. 48 règle le droit d'accès aux données stockées dans le MID et le droit de rectification et d'effacement de ces dernières. Si une personne demande si des données personnelles sont traitées à son sujet ou qu'elle veut demander la rectification ou l'effacement de données ou limiter leur traitement, elle peut s'adresser à l'autorité compétente de n'importe quel État Schengen, qui examinera sa demande et y répondra. Si la demande est adressée à un État qui n'est pas compétent en la matière, ce dernier prendra contact avec l'État Schengen compétent, ou avec l'unité centrale ETIAS si c'est elle qui est chargée de la vérification, afin de vérifier les données. Cette vérification doit en général avoir lieu dans les 45 jours suivant la réception de la demande, mais une prolongation est possible. La personne concernée est informée par écrit du résultat de la vérification et de l'éventuelle correction ou de l'éventuel effacement de ses données. Si l'État chargé de l'examen est d'avis que les données n'ont pas été traitées ou enregistrées de manière illicite, il en informe la personne concernée et lui indique également des modalités de plainte ou de recours. L'ensemble du processus doit être consigné par écrit. Un nouveau portail en ligne doit permettre aux personnes concernées de faire valoir plus facilement leur droit d'accès aux données à caractère personnel et leur droit de rectification, d'effacement ou de limitation du traitement de ces dernières et d'entrer en contact avec les autorités compétentes (art. 49). Le numéro d'identification unique au sens de l'art. 34*c* permet notamment de connaître l'autorité compétente. Le portail en ligne contient également un modèle de courriel destiné à faciliter la communication et à obtenir des informations sur les droits et les procédures.

Les données à caractère personnel stockées et traitées dans les composants centraux ne peuvent en principe pas être transférées vers un pays tiers, une organisation internationale, une entité privée ou une personne physique ou être mises à leur disposition (art. 50). Conformément à l'art. 50, cette règle s'applique sous réserve des dispositions en matière de protection des données concernant le transfert de données dans les bases juridiques des systèmes de l'UE ainsi que l'interrogation des données d'Interpol via l'ESP conformément aux règlements de l'UE sur l'interopérabilité.

Les art. 51 et 52 règlent le contrôle par les autorités de surveillance ainsi que les audits par le Contrôleur européen de la protection des données. Les États Schengen doivent veiller à ce que les autorités de surveillance contrôlent en toute indépendance la licéité du traitement des données. À cet effet, ils doivent s'assurer que les autorités de contrôle disposent de ressources et d'expertise suffisantes et leur communiquer toutes les informations nécessaires au contrôle. Les autorités de contrôle sont tenues de publier chaque année le nombre de demandes visant à faire rectifier ou effacer des données à caractère personnel ou à en faire limiter le traitement, ainsi que les mesures prises par la suite. Elles réalisent tous les 4 ans au minimum un audit des opérations de traitement conformément aux normes internationales d'audit applicables. Le Contrôleur européen de la protection des données est chargé de contrôler les opérations de traitement des données de l'eu-LISA, de l'unité centrale ETIAS et d'Europol. Les autorités de contrôle nationales et le Contrôleur européen de la protection des données coopèrent activement et assurent un contrôle coordonné de l'utilisation des composants centraux et de l'application d'autres dispositions des règlements sur l'interopérabilité (art. 53). Tous les 2 ans, le Contrôleur européen de la protection des données réalise un rapport d'activités conjoint. Ce rapport comporte un chapitre sur chaque État Schengen, établi par l'autorité de contrôle de l'État membre concerné.

Responsabilités (chap. VIII)

Jusqu'à l'art. 57, les deux règlements sur l'interopérabilité sont identiques. Les art. 54 et 55 décrivent les responsabilités de l'eu-LISA durant la phase de conception et de développement et après la mise en service. L'eu-LISA est chargée du développement des composants centraux, des adaptations nécessaires pour établir l'interopérabilité entre les systèmes centraux de l'EES, du VIS, d'ETIAS, du SIS, d'Eurodac et de l'ECRIS-TCN et de l'infrastructure de communication. Après la mise en service, l'eu-LISA assure le bon fonctionnement des systèmes et se charge de leur gestion technique et leur maintenance, tout en n'ayant accès à aucune donnée à caractère personnel. L'art. 56 établit la liste des responsabilités des États Schengen. Ces dernières comprennent notamment la connexion des systèmes nationaux aux nouveaux composants centraux et la gestion et les modalités de l'accès des autorités nationales autorisées à l'ESP, au CIR et au MID. Le règlement IOP Police énumère à l'art. 57 les responsabilités d'Europol. Les responsabilités de l'unité centrale ETIAS (art. 57 du règlement IOP Frontières, art. 58 du règlement IOP Police) sont formulées de manière identique dans les deux règlements.

Modifications d'autres instruments de l'Union (chap. IX)

Les règlements de l'UE sur l'interopérabilité entraînent des modifications d'autres actes juridiques. Il s'agit d'actes juridiques que la Suisse a déjà repris au moyen d'un échange de notes ou pour lesquels une procédure de reprise est en cours, à savoir le règlement (CE) n° 767/2008 sur le VIS, le règlement (UE) 2016/399 sur le code frontières Schengen[28], le règlement (UE) 2017/2226 sur l'EES[29], le règlement (UE) 2018/1240 sur ETIAS[30], le règlement (UE) 2018/1726 sur l'eu-LISA[31], le règlement (UE) 2018/1861 sur le SIS[32], la décision 2004/512/CE sur la mise en place du VIS[33] et la décision 2008/633/JAI concernant l'accès des autorités de poursuite pénale au VIS[34]. Les modifications de ces actes sont réglées séparément aux art. 58 à 65 du règlement IOP Frontières. Le règlement IOP Police présente aux art. 59 à 62 les modifications du règlement (UE) 2018/1726 sur l'eu-LISA, du règlement (UE) 2018/1862 sur le SIS et du règlement (UE) 2019/816 sur l'ECRIS-TCN[35]. La Suisse n'est cependant pas liée par ce dernier.

28 Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), JO L 77 du 23.3.2016, p. 1.

29 Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011, JO L 327 du 9.12.2017, p. 20; modifié en dernier lieu par le règlement (UE) 2019/817, JO L 135 p. 27.

30 Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226, JO L 236 du 19.9.2018, p. 1; modifié en dernier lieu par le règlement (EU) 2019/817, JO L 135 du 22.5.2019, p. 27.

31 Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011, JO L 295 du 21.11.2018, p. 99.

32 Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 1987/2006, JO L 312 du 7.12.2018, p. 14.

33 Décision du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS), JO L 213 du 15.6.2004, p. 5.

34 Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 218 du 13.8.2008, p. 129.

35 Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726, JO L 135 du 22.5.2019, p. 1.

Ces modifications des actes précités sont nécessaires pour exploiter pleinement les nouvelles possibilités qu'offre l'interopérabilité. Elles visent en particulier à définir les catégories de données qui seront stockées ou saisies dans les composants centraux et à prévoir la connexion des différents systèmes aux nouveaux composants centraux.

Dispositions finales (chap. X)

Ce dernier chapitre contient des dispositions concernant les périodes transitoires pour l'utilisation des différents composants centraux, ainsi que les tâches des différentes autorités qui doivent être remplies pendant celles-ci (art. 67 à 69 du règlement IOP Frontières et art. 63 à 65 du règlement IOP Police). Sont également réglés dans ces chapitres la mise en service (art. 72 du règlement IOP Frontières et art. 68 du règlement IOP Police), la formation des autorités compétentes (art. 76 du règlement IOP Frontières et art. 72 du règlement IOP Police), le suivi et l'évaluation du développement et du fonctionnement des composants centraux (art. 78 du règlement IOP Frontières et art. 74 du règlement IOP Police) et l'entrée en vigueur (art. 79 du règlement IOP Frontières et art. 75 du règlement IOP Police).

6 Présentation de l'acte de mise en œuvre

6.1 Réglementation proposée

Le projet porte sur la reprise de développements de l'acquis de Schengen. Leur transposition dans le droit suisse nécessite une modification de lois fédérales et, plus tard, des ordonnances qui s'y rapportent (cf. ch. 6.2).

6.2 Nécessité des adaptations proposées

Les règlements IOP Frontières et IOP Police contiennent tant des dispositions directement applicables que des dispositions qui doivent être transposées dans le droit interne. L'arrêté fédéral ne répète les dispositions des règlements de l'UE que dans la mesure où la LPD l'impose. Ainsi, les buts du traitement des données, les droits d'accès, la transmission de données et la sanction en cas de traitement abusif de données doivent être réglés dans une loi au sens formel. De plus, certaines dispositions nécessaires à la compréhension du contexte sont répétées, par exemple la définition des composants de l'interopérabilité.

Le présent chapitre détaille les nouveautés requérant une modification de lois fédérales. De nombreux changements n'ont toutefois de conséquences qu'au niveau des ordonnances qu'il faudra édicter ultérieurement et ne sont donc pas exposés ci-après. Les règlements européens sur l'interopérabilité n'étendront pas les droits d'accès des différentes autorités aux systèmes sous-jacents ni ne changeront les finalités des accès. Le portail en ligne créera en revanche de nouvelles possibilités qui faciliteront la communication entre les autorités nationales compétentes sur les personnes enregistrées. L'accès à des données sensibles restera donc clairement réglementé, même après la reprise des deux règlements européens.

Les composants centraux relient les systèmes d'information régis par la LEI et les banques de données de police régies par la LSIP. Par souci de transparence, ils doivent être réglementés en conséquence dans ces deux lois, puisqu'elles contiennent la base légale au sens formel sur laquelle reposent les systèmes d'information concernés. Les dispositions sont présentées dans l'ordre correspondant à la mise en service prévue des différents composants (le sBMS d'abord, suivi du CIR, de l'ESP et du MID). L'introduction des composants centraux entraîne par ailleurs des adaptations dans la structure de la LEI comme dans celle de la LSIP.

Les modifications concrètes de chacune des lois sont résumées ci-après (cf. ch. 7 pour le commentaire des dispositions).

Loi fédérale sur les étrangers et l'intégration

Le terme de « systèmes d'information Schengen-Dublin » est introduit parce que certains systèmes d'information réglementés dans la LEI sont régis par l'AAD et pour éviter toute confusion avec la partie nationale du Système d'information Schengen (N-SIS).

Les chapitres 14 à 14*c* LEI doivent être réorganisés eu raison de l'introduction des composants centraux des systèmes d'information Schengen-Dublin. L'un de ces chapitres contiendra les dispositions générales sur la protection des données; un autre réglementera l'ensemble des systèmes d'information; un autre encore portera sur les règles relatives à l'interopérabilité entre les systèmes d'information Schengen-Dublin; enfin, un chapitre sera consacré aux dispositions concernant la protection des données dans le domaine Schengen-Dublin.

Étant donné que neuf règlements de l'UE ont dû être modifiés en vue de la mise en place de l'interopérabilité, les dispositions correspondantes de la LEI qui régissent les systèmes d'information Schengen-Dublin – ou qui seront appelés à le faire – doivent être modifiées elles aussi.

Le CIR fait désormais partie intégrante de l'EES, d'ETIAS et du VIS (et, ultérieurement, d'Eurodac). Les dispositions correspondantes de la LEI doivent être modifiées, car le CIR remplacera une partie du système central des différents systèmes d'information de l'UE de telle sorte que des données alphanumériques (données d'identité et données relatives aux documents de voyage) et biométriques des différents systèmes seront désormais enregistrées dans le CIR. Ainsi, la LEI doit préciser quelles données resteront stockées dans le système central de chacun des systèmes d'information concernés et lesquelles seront désormais stockées dans la partie du CIR.

En outre, les différents composants de l'interopérabilité doivent être réglementés. L'art. 17, al. 1, LPD, prévoit en effet que les organes fédéraux ne peuvent traiter des données personnelles que s'il existe une base légale formelle. En particulier, le contenu des différents composants doit être défini et les règles d'accès doivent être fixées (sBMS à l'art. 110, CIR aux art. 110*a* à 110*d* et MID à l'art. 110*f*).

Dans le cas du CIR, les accès doivent être réglementés en fonction de leur finalité: identification à l'art. 110*b*, détection d'identités multiples à l'art. 110*c* et détection d'infractions pénales à l'art. 110*d*. Dans ce dernier cas, les autorités désignées, en

particulier le Service de renseignement de la Confédération (SRC), doivent toutes pouvoir vérifier dans le CIR si des données figurent dans un des systèmes d'information Schengen-Dublin ne relevant pas du domaine de la police (EES, ETIAS, VIS) (mécanisme « réponse positive / pas de réponse positive » conformément à l'art. 22 des règlements de l'UE sur l'interopérabilité). La loi doit également désigner les autorités policières qui ont accès au système à des fins d'identification et préciser quelle autorité est responsable de la vérification des identités multiples et dans quels cas.

La consultation de données par l'ESP (art. 110*e*) et les différents droits d'accès au MID (art. 110*g*) par les autorités compétentes doivent également être réglementés.

La communication de données (art. 110*h*), la responsabilité du traitement des données dans le sBMS, le CIR et le MID, ainsi que les sanctions en cas d'utilisation abusive des données doivent également être prévues dans la loi (art. 120*d*). À cet égard, les dispositions actuelles concernant le système central d'information sur les visas (C-VIS), l'EES et ETIAS doivent être modifiées.

Il faut s'attendre à d'autres précisions dans les actes d'exécution et les actes délégués de l'UE, actes qui seront notifiés à la Suisse en temps voulu et qui devraient également être mis en œuvre au niveau de l'ordonnance.

Enfin, les renvois aux règlements européens dans la loi doivent être mis à jour.

Loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile

Dans la loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA)[36], certains renvois à des dispositions de la LEI touchées par la présente révision doivent être modifiés. Ces adaptations n'entraînent aucune modification matérielle de la LDEA.

Loi sur la responsabilité

Actuellement, la loi fédérale du 14 mars 1958 sur la responsabilité (LRCF)[37] réglemente la responsabilité des dommages découlant de l'exploitation du SIS aux art. 19*a* et 19*b*. Les bases juridiques européennes de l'EES, du VIS, d'ETIAS et des éléments centraux contiennent des dispositions sur la responsabilité similaires, en cas de dommage causé par un traitement illicite des données, à celles qui s'appliquent déjà au SIS. Il est donc indiqué de réglementer dans la LRCF tous les systèmes d'information Schengen-Dublin et leurs composants qui sont soumis à des dispositions sur la responsabilité. Le sBMS et l'ESP ne sont cependant pas un assemblage de données au sens de l'art. 3, let. d, LPD puisqu'aucune donnée personnelle n'y figure. Le terme « composant » vient donc compléter celui de « système d'information ».

36 RS **142.51**
37 RS **170.32**

Loi fédérale sur les systèmes d'information de police de la Confédération

La LSIP, qui régit les bases juridiques des systèmes d'information de police de la Confédération, doit également être modifiée. Ici aussi, la plupart des dispositions des deux règlements de l'UE sur l'interopérabilité sont directement applicables et ne nécessitent pas de transposition dans le droit suisse. En vertu de l'art. 17 LPD, les autorités fédérales ne peuvent traiter les données sensibles que si une loi au sens formel le prévoit expressément. Les éléments centraux qui portent sur les systèmes d'information Schengen-Dublin réglementés dans la LSIP, à savoir les éléments centraux qui englobent le SIS, doivent donc y être inscrits.

Des dispositions régissant le sBMS, l'ESP et le MID, largement analogues à celles contenues dans la LEI, sont ainsi introduites dans la LSIP.

Les dispositions régissant les systèmes d'information Schengen-Dublin ou leurs composants ainsi que le traitement des données qu'ils contiennent et la responsabilité de ce traitement figurent dans des articles consécutifs (art. 16 à 16*f* LSIP), dans l'ordre correspondant à la mise en service prévue (le sBMS à l'art. 16*a*, l'ESP à l'art. 16*b* et le MID à l'art. 16*c*). Le projet ne remanie davantage la structure de la LSIP, cette dernière étant déjà en cours de modification dans le cadre d'autres projets de lois (loi fédérale sur les mesures policières de lutte contre le terrorisme[38] et arrêté fédéral portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases juridiques concernant l'établissement, le fonctionnement et l'utilisation du système d'information Schengen [SIS][39]). À l'heure actuelle, l'ordre de l'entrée en vigueur de tous ces projets n'est pas encore défini. Étant donné que la LSIP fera prochainement l'objet d'une révision totale, il n'est pas opportun d'en adapter la systématique.

Depuis l'entrée en vigueur le 1er mars 2019 de la loi fédérale mettant en œuvre la directive (UE) 2016/680 l'art. 349*c* du code pénal (CP)[40] réglemente la communication de données personnelles à un État tiers ou à un organisme international[41]. Dans la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)[42], l'art. 13, al. 2, lui aussi en vigueur depuis le 1er mars 2019, stipule que la communication de données personnelles dans le cadre de la coopération policière avec des autorités de poursuite pénale étrangères s'aligne sur les art. 349*a* à 349*h* CP[43]. La LSIP régit quant à elle de manière générale l'utilisation de systèmes d'information de police de la Confédération; elle sera encore élargie dans le sillage de la mise en œuvre des règlements européens sur l'interopérabilité. La communication de données à des tiers et à des organisations internationales dans le domaine de l'interopérabilité doit donc être régie dans une disposition distincte (art. 16*e*). La responsabilité du traitement des données dans les systèmes

38 FF **2019** 4639
39 FF **2020** ....
40 RS **311.0**
41 RO **2019** 625
42 RS **360**
43 RO **2019** 625

d'information Schengen-Dublin ou leurs composants doit elle aussi être réglementée (art. 16*f*).

6.3 Besoin particulier de coordination

Le présent projet requiert une coordination particulière dans la perspective de la reprise et de la mise en œuvre des bases légales portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS). Le projet ETIAS[44] étant actuellement traité par le Parlement, le présent projet d'arrêté fédéral ne peut en effet pas se référer à ce système d'information, bien qu'il fasse partie intégrante de l'interopérabilité. Il y a aussi un besoin de coordination en ce qui concerne la reprise des bases juridiques sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS), le projet SIS[45] étant lui aussi actuellement traité par le Parlement. Après les votes finaux, les articles concernés du présent projet d'arrêté fédéral devront être complétés ou adaptés en conséquence. Par ailleurs, le présent projet doit être coordonné avec la reprise des bases juridiques portant création d'un système d'entrée et de sortie (EES)[46]. Un éventuel besoin de coordination doit être aussi assuré avec la LEI modifiée le 14 décembre 2018 relative à la mise en œuvre des normes procédurales et des systèmes d'information[47]. Le besoin de coordination entre les différents projets est expliqué en détail au chap. 8.

44 Message du 6 mars 2020 relatif à l'approbation et à la mise en œuvre de l'échange de notes entre la Suisse et l'UE sur la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'information et d'autorisation et concernant les voyages (ETIAS) (développement de l'acquis de Schengen) et à la modification de la loi fédérale sur les étrangers et l'intégration (Assujettissement du Service de renseignement de la Confédération à la loi sur la protection des données Schengen), FF **2020** 2885

45 Message du 6 mars 2020 relatif à l'approbation et à la mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases légales concernant l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) (développements de l'acquis de Schengen) et à la modification de la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile, FF **2020** 3465

46 Arrêté fédéral portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases juridiques en vue de la création et de l'utilisation du système d'entrée et de sortie (EES) (règlements [UE] 2017/2226 et 2017/2225) (Développements de l'acquis de Schengen), FF **2019** 4397

47 RO **2019** 1413, FF **2018** 1673

7 Commentaire des dispositions de l'acte de mise en œuvre

7.1 Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)

Art. 7, al. 3, 1re phrase, note de bas de page

Étant donné que le règlement (UE) 2016/399 sur le code frontières Schengen est modifié par le règlement IOP Frontières, la note de bas de page figurant à l'art. 7, al. 3 doit être adaptée.

Art. 9a

L'art. 9*a* reprend sans modification matérielle le contenu de l'art. 103. Il traite de la surveillance de l'arrivée à l'aéroport. Ce changement implique une modification des renvois qui figurent à l'art. 1, al. 2, LDEA.

Art. 92a

L'art. 92*a* reprend sans modification matérielle le contenu de l'art. 104. Il traite de l'obligation des entreprises de transport aérien de communiquer des données personnelles. Ce changement implique une modification des renvois qui figurent aux art. 104*a*, al. 1bis à 5, 104*b*, al. 1, 122*b*, al. 2 et 122*c*, al. 3, let. b.

Chapitre 14 Traitement et protection des données

La mise en place des nouveaux composants centraux ayant une incidence sur l'ensemble des systèmes d'information Schengen-Dublin entraîne une réorganisation des chap. 14 à 14*c*:

- le chap. 14 contient désormais toutes les dispositions relatives à la protection et au traitement des données en général;
- le chap. 14*a* réglemente désormais tous les systèmes d'information (les systèmes nationaux et les systèmes d'information Schengen-Dublin);
- le chap. 14*b*, qui portait jusqu'à présent sur la protection des données dans le cadre des accords d'association à Schengen, contient désormais les dispositions relatives à l'interopérabilité entre les systèmes d'information Schengen-Dublin;
- le chap. 14*c*, qui portait jusqu'à présent sur Eurodac, contient désormais les dispositions relatives à la protection des données dans le cadre des accords d'association à Schengen; les dispositions relatives à Eurodac sont désormais incluses dans le chap. 14*a*, dans une section à part.

Le chap. 14 voit son titre modifié. Il ne réglemente désormais plus que le traitement et la protection des données. Les systèmes d'information sont désormais traités dans un chapitre à part (chap. 14*a*).

En plus des art. 101 (Traitement des données), 102 (Collecte de données à des fins d'identification et de détermination de l'âge), 102*a* (Données biométriques pour titres de séjour) et 102*b* (Contrôle de l'identité du détenteur d'un titre de séjour biométrique), le chap. 14 comprend trois nouveaux articles:

- un art. 102*c* (Communication de données personnelles à l'étranger);
- un art. 102*d* (Communication de données personnelles à l'État d'origine ou de provenance);
- un art. 102*e* (Communication de données personnelles dans le cadre des accords de réadmission et de transit).

La subdivision en sections est supprimée.

Art. 102c Communication de données personnelles à l'étranger

L'art. 102*c* reprend sans modification matérielle le contenu de l'art. 105. Il traite de la communication de données personnelles à l'étranger.

Art. 102d Communication de données personnelles à l'État d'origine ou de provenance

L'art. 102*d* reprend sans modification matérielle le contenu de l'art. 106. Il traite de la communication de données personnelles à l'État d'origine ou de provenance.

Art. 102e Communication de données personnelles dans le cadre des accords de réadmission et de transit

L'art. 102*e* reprend sans modification matérielle le contenu de l'art. 107. Il traite de la communication de données personnelles dans le cadre des accords de réadmission et de transit.

Art. 103

Cf. commentaire relatif à l'art. 9*a*.

Chapitre 14a Systèmes d'information

Le chapitre 14*a* débute désormais avant l'art. 103*a* (Système d'information sur les refus d'entrée, ci-après « système INAD »). Il traite des systèmes d'information suivants:

- Section 1 (système INAD): art. 103*a*[48];
- Section 2 (Système d'entrée et de sortie [EES] et contrôle automatisé à la frontière): art. 103*b* à 103*g*[49];

48 FF **2019** 4397
49 FF **2019** 4397

- Section 3 (Système d'information sur les passagers [système API]): art. 104*a* à 104*c* et 108 (l'art. 108 étant déjà abrogé);
- Section 4 (Système central d'information sur les visas [C-VIS] et système national d'information sur les visas [ORBIS]): art. 109*a* à 109*e*;
- Section 5 (Système d'information destiné à la mise en œuvre des retours): art. 109*f* à 109*j*;
- Section 6 (Eurodac): art. 109*k* et 109*l*;
- Section 7 (Système de gestion des dossiers personnels et de la documentation): art. 109*m*.

Section 1 Système d'information sur les refus d'entrée (système INAD)

Une section intitulée *Système d'information sur les refus d'entrée (système INAD)* est ajoutée avant l'art. 103*a*.

Art. 103a[50]

Le titre de l'art. 103*a* peut être supprimé puisque la section 1 ne comporte plus qu'un seul article.

Section 2 Système d'entrée et de sortie (EES) et contrôle automatisé à la frontière

Une nouvelle section est créée avant l'art. 103*b*. Elle comporte des dispositions relatives au système EES et au contrôle automatisé à la frontière.

Art. 103b, al. 1, note de bas de page, 2, let. a et b[bis]*, et 4*[51]

Al. 1, note de bas de page

Le règlement (UE) 2017/2226 portant création du système EES étant modifié par le règlement IOP Frontières, la note de bas de page de l'art. 103*b*, al. 1, doit être modifiée.

Al. 2, let. a et b[bis]

L'art. 103*b*, al. 2, let. a, n'énumère plus les données relatives aux visas délivrés. Ces données sont désormais définies à part à la let. b[bis], ce qui permet de faire. un renvoi précis, à l'al. 4, aux données désormais stockées dans le CIR. L'expression *données alphanumériques* est remplacée par *données d'identité et données du document de voyage*.

50 FF **2019** 4397
51 FF **2019** 4397

Al. 4

L'al. 4 précise quelles données sont stockées dans le CIR (cf. commentaire relatif à l'art. 110*a*). Les données d'identité et les données du document de voyage (art. 103*b*, al. 2, let. a), de même que la photographie et, éventuellement, les empreintes digitales (art. 103*b*, al. 2, let. b, et 3) sont conservées dans le CIR. Les informations concernant les dates d'entrée et de sortie de l'espace Schengen, le point de passage frontalier, l'autorité responsable du contrôle aux frontières et les données relatives aux refus d'entrée ne sont pas enregistrées dans le CIR ; elles continuent de n'être stockées que dans l'EES.

Art. 103d, titre (ne concerne que le texte français) et al.3[52]

La formulation du titre de l'article en français est harmonisée avec celle de la disposition. En ce qui concerne la communication de données de l'EES qui sont stockées dans le CIR, l'al. 3 renvoie à l'art. 110*h*, lequel renvoie à son tour à l'art. 40 des deux règlements de l'UE sur l'interopérabilité (cf. commentaire relatif à l'art. 110*h* et ch. 3.2 Protection des données). De manière générale, s'agissant des données de base EES enregistrées dans le CIR, les dispositions qui s'appliquent sont celles du chapitre VII des règlements de l'UE sur l'interopérabilité.

Art. 104

Cf. commentaire relatif à l'art. 92*a*.

Section 3 Système d'information sur les passagers (système API) et accès aux données relatives aux passagers dans des cas particuliers

Une nouvelle section est créée avant l'art. 104*a*. Elle contient les dispositions relatives au système d'information sur les passagers API (art. 104*a* à 104*c*). Certaines dispositions de cette section subissent des modifications d'ordre formel. Aucune modification matérielle n'y est apportée.

Art. 104a, titre et al. 1bis *à 5, partie introductive*

Comme l'art. 104*a* est désormais l'une des nombreuses dispositions de la section consacrée au système d'information sur les passagers, il est nécessaire de modifier le titre de cette disposition. En outre, les renvois figurant dans certains alinéas de cet article doivent être modifiés (cf. commentaire relatif à l'art. 92*a*).

Art. 104b, al. 1

Cf. commentaire relatif à l'art. 92*a*.

52 FF **2019** 4397

Chap. 14, section 3 (art. 105 à 107)

La section 3 du chapitre 14 est abrogée. Ce dernier n'est plus subdivisé en sections. La teneur des art. 105 à 107 ne subit pas de modification matérielle et figure désormais aux art. 102*c* à 102*e*.

Section 4 Système central d'information sur les visas (C-VIS) et système national d'information sur les visas (ORBIS)

Une nouvelle section est créée avant l'art. 109*a*. Elle contient les règles applicables au C-VIS et à ORBIS (art. 109*a* à 109*e* et 109*f* à 109*j*).

Art. 109a, titre et al. 1 et 1bis

Al. 1

Étant donné que le règlement (CE) n° 767/2008 concernant le VIS a été modifié par le règlement IOP Frontières, la note de bas de page de l'art. 109*a*, al. 1, doit être modifiée.

Al. 1bis

L'al. 1bis précise quelles données sont stockées dans le C-VIS et lesquelles sont stockées dans le CIR (cf. commentaire relatif à l'art. 110*a*). Sont ainsi stockées dans le CIR les données d'identité, les données du document de voyage et les données biométriques. Les autres informations sur la procédure d'octroi de visas ne sont pas enregistrées dans le CIR; elles continuent de n'être stockées que dans le C-VIS.

Art. 109b, al. 1, 2, phrase introductive, et 2bis à 4

L'abréviation du système national d'information sur les visas, ORBIS, est introduite à l'al. 1. En conséquence, dans les dispositions suivantes, *système national d'information sur les visas* est remplacé par *ORBIS*. Quelques adaptations formelles sont par ailleurs apportées à diverses dispositions.

Art. 109c, titre et phrase introductive

Cf. commentaire relatif à l'art. 109*b*.

Art. 109d, note de bas en page

La note de bas de page doit être mise à jour.

Section 5 Système d'information destiné à la mise en œuvre des retours

Une nouvelle section est créée avant l'art. 109*f* LEI. Elle contient les règles relatives au système d'information pour la mise en œuvre des retours. Ces dispositions ont été introduites lors de la modification de la LEI du 14 décembre 2018 relative aux

normes procédurales et systèmes d'information et sont entrées en vigueur le 1er avril 2020[53]. Aucune modification matérielle n'y est apportée.

Section 6 Eurodac

Une nouvelle section est créée avant l'art. 109*k*. Elle contient les règles concernant Eurodac.

Art. 109k Saisie et transmission de données dans Eurodac

L'art. 109*k* reprend le contenu de l'art. 111*i* sans aucune modification matérielle. Seul le titre est modifié. Cet article concerne Eurodac.

Les composants centraux devraient également couvrir Eurodac. Par exemple, le CIR devrait inclure une unité de stockage commune pour les données d'identité, les données biométriques et les données du document de voyage des personnes enregistrées dans Eurodac. Toutefois, le règlement IOP Police ne s'applique à Eurodac qu'à compter de la date d'application de la nouvelle version du règlement (UE) n° 603/2013 (art. 75 du règlement IOP Police).

Art. 109l Communication de données stockées dans Eurodac

Cet article reprend l'art. 111*d*, al. 5, sans modification matérielle, mais avec des ajustements d'ordre rédactionnel. Cette disposition régit la communication des données Eurodac et relève thématiquement de la section 7.

Section 7 Système de gestion des dossiers personnels et de la documentation

La section 3 devient la section 8 et contient une disposition sur le système de gestion des dossiers personnels et de la documentation du Secrétariat d'État aux migrations (SEM).

Art. 109m

Cet article reprend l'art. 110 sans aucune modification matérielle.

Chapitre 14b Interopérabilité des systèmes d'information Schengen-Dublin

Section 1 Service partagé d'établissement de correspondances biométriques (sBMS)

Art. 110

L'art. 110 réglemente désormais le service partagé pour la comparaison des données biométriques (sBMS). Les dispositions qui étaient contenues dans l'actuel art. 110

53 RO **2019** 1413, **2020** 881

(système automatisé de gestion des dossiers personnels et de la documentation) ne sont plus nécessaires et sont donc abrogées.

Al. 1 et 3

Le sBMS permet de consulter les systèmes d'information Schengen-Dublin concernés par l'interopérabilité des systèmes au moyen de modèles biométriques (*templates*) générés à partir de données biométriques à caractère personnel dans les systèmes d'information Schengen-Dublin. Ces modèles ne permettent pas d'en déduire les données biométriques réelles.

Contrairement au CIR (art. 110*a* à 110*d*) ou au MID (art. 110*g*), le sBMS ne constitue pas un fichier, c'est-à-dire un ensemble de données, au sens de l'art. 3, let. g, LPD. Les modèles biométriques contenus dans le sBMS ne sont en effet pas des données biométriques à caractère personnel et aucune autre donnée personnelle n'est stockée dans ce système (cf. ch. 5.2.1). Par souci d'exhaustivité, la LEI doit contenir une disposition relative au sBMS, même si les dispositions relatives au sBMS des deux règlements de l'UE sur l'interopérabilité sont directement applicables. D'autres nouvelles dispositions de la LEI comportent par ailleurs un renvoi au sBMS.

Al. 2

La référence dans le sBMS au système d'information concerné sert à déterminer de quel système d'information Schengen-Dublin (EES, VIS, Eurodac, SIS) et de quels enregistrements figurant dans ces systèmes d'information proviennent les données biométriques à caractère personnel sur la base desquelles les modèles biométriques ont été produits.

Les règles détaillées relatives au sBMS figurent au chapitre III des deux règlements de l'UE sur l'interopérabilité. Le ch. 5.1.2 fournit des informations détaillées sur le sBMS.

Section 2 Répertoire commun de données d'identité (CIR)

Art. 110a Contenu du répertoire commun de données d'identité

Al. 1

Pour chaque personne enregistrée dans l'EES, le VIS, ETIAS ou, à un stade ultérieur, dans Eurodac, le CIR gère un fichier individuel contenant les données d'identité, les données du document de voyage et les données biométriques extraites de ces systèmes d'information Schengen-Dublin. Les données alphanumériques comprennent les données d'identité de la personne concernée et les données du document de voyage. ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8.1).

Le CIR est destiné à faciliter l'identification des personnes dont les données sont contenues dans les systèmes d'information Schengen-Dublin susmentionnés et la détection des identités multiples. Il doit également faciliter et harmoniser l'accès à

ces systèmes d'information pour les autorités désignées, à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'investigation en la matière. Les droits d'accès correspondants au CIR sont régis par les art. 110*b* à 110*d*. Il est prévu que la consultation du CIR passe par l'ESP (cf. art. 110*e*). Le CIR devrait entrer en service à l'été 2022, tandis que l'ESP ne sera opérationnel qu'en milieu d'année 2023. Il reste donc à déterminer si, jusqu'à ce que les deux composants centraux soient opérationnels, le CIR pourra être consulté sans l'ESP pendant une période transitoire ou non. Des informations détaillées sur le CIR figurent au ch. 5.1.

Al. 2

Pour chaque ensemble de données d'identité, de données du document de voyage et de données biométriques stockées, le CIR contient une référence au système d'information Schengen-Dublin sous-jacent d'où proviennent les données ainsi qu'une référence à l'ensemble des enregistrements contenus dans le système d'information Schengen-Dublin correspondant.

Les règles détaillées relatives au CIR figurent au chapitre IV des deux règlements de l'UE sur l'interopérabilité.

Art. 110b Consultation du CIR à des fins d'identification

Al. 1 et 2

Conformément à l'art. 20, par. 1, des règlements de l'UE sur l'interopérabilité, une consultation ne peut être menée à des fins d'identification que si l'une des conditions suivantes est remplie (par. 1, let. a, et 2):

- une autorité policière n'est pas en mesure d'identifier une personne en raison de l'absence d'un document de voyage ou d'un autre document crédible prouvant l'identité de cette personne;
- un doute subsiste au sujet des données d'identité fournies par une personne;
- un doute subsiste au sujet de l'authenticité du document de voyage ou d'un autre document crédible fourni par une personne;
- un doute subsiste au sujet de l'identité du titulaire d'un document de voyage ou d'un autre document crédible;
- une personne n'est pas en mesure de coopérer ou refuse de le faire.

En cas de catastrophe naturelle, d'accident ou d'attentat, les autorités chargées d'effectuer des recherches dans le système en vertu de l'art. 110*b*, al. 3, ne peuvent utiliser le CIR que pour identifier, au moyen des données biométriques de l'intéressé, une personne inconnue qui ne peut décliner son identité ou des restes humains non identifiables par un autre moyen (al. 1, let b).

Al. 3

L'al. 3 détermine quelles sont les autorités habilitées à mener des recherches dans le CIR, dans des cas particuliers, afin d'identifier des ressortissants d'États tiers. Cette consultation du CIR est autorisée uniquement aux fins suivantes: pour lutter contre l'immigration clandestine, pour garantir la sécurité publique, pour préserver l'ordre public et pour sauvegarder la sécurité intérieure.

Les autorités compétentes sont l'Office fédéral de la police (fedpol), les autorités de police des cantons et des communes et l'Administration fédérale des douanes (AFD), afin de garantir la sécurité intérieure et de protéger la population. fedpol obtient l'accès pour mener sur le territoire national les identifications liées à ses tâches de maintien de l'ordre et de la sécurité publics. Les autorités de police des cantons et des communes disposent également d'un accès au CIR pour vérifier la légalité du séjour de personnes. L'AFD peut accéder au CIR pour exécuter les tâches qui lui ont été confiées, en particulier pour garantir la légalité de la circulation des personnes et des marchandises traversant la frontière douanière et pour contribuer à la sécurité intérieure du pays et à la protection de la population. Elle est notamment habilitée à contrôler la circulation des personnes. Ce contrôle porte sur l'identité des personnes concernées, leur droit de franchir la frontière et leur droit de séjourner en Suisse.

Al. 4 et 5

Les recherches dans le CIR sont généralement effectuées en se fondant sur les données biométriques du ressortissant étranger prélevées directement sur place . La procédure d'identification doit en principe être lancée en présence de la personne concernée. La présence de cette dernière n'est cependant pas nécessaire pendant toute la durée de la procédure. Si une recherche au moyen de données biométriques est impossible ou si elle n'aboutit pas, les données du document de voyage ou les données d'identité sont utilisées.

Art. 110c Consultation du CIR à des fins de détection d'identités multiples

Al. 1

Si un lien jaune apparaît lors d'une recherche dans le CIR (cf. ch. 5.1.4), les autorités visées par cet alinéa ont uniquement accès, aux fins de la vérification manuelle des différentes identités, aux données biométriques à caractère personnel contenues dans le CIR, aux données d'identité, aux données du document de voyage et à la référence au système d'information Schengen-Dublin dont proviennent ces données. ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8).

Al. 2

Si un lien rouge apparaît lors d'une recherche dans le CIR (cf. ch. 5.1.4), les autorités ayant accès au CIR, à l'EES, à ETIAS, au C-VIS, à Eurodac ou au SIS en vertu de la LEI ou de la LSIP peuvent accéder aux données contenues dans le CIR et à la référence au système d'information Schengen-Dublin afin de lutter contre

l'usurpation d'identité (cf. commentaire relatif à l'art. 1). ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8.1).

Art. 110d Consultation du CIR à des fins de prévention ou de détection d'infractions terroristes ou d'autres infractions pénales graves ou d'investigations en la matière

Al. 1 et 2

Si, dans un cas particulier, des éléments indiquent que la consultation d'un système d'information Schengen-Dublin peut contribuer à détecter ou à prévenir des infractions terroristes ou d'autres infractions pénales graves ou permettre d'investiguer en la matière, fedpol, le SRC, le Ministère public de la Confédération, les autorités cantonales de police et de poursuite pénale, de même que les autorités de police des villes de Zurich, Winterthour, Lausanne, Chiasso et Lugano peuvent consulter le CIR afin de déterminer si l'EES, le VIS, ETIAS ou Eurodac contiennent des données sur la personne concernée. Les autorités de police communales énumérées dans cet alinéa sont autorisées à consulter ces données parce que, à l'instar des polices cantonales, elles exercent des missions de police criminelle liées à la prévention et à la détection des infractions pénales graves et aux investigations à mener en la matière (cf. réglementation figurant à l'art. 109*a*, al. 3).

Le terme d'infraction grave est défini de façon détaillée dans le message du 22 mai 2019 concernant la loi fédérale sur les mesures policières de lutte contre le terrorisme[54]. Sont notamment considérées comme infractions graves les infractions visées à l'art. 286, al. 2, du code de procédure pénale[55]. Dans le cadre des modifications de loi en vue de combattre le terrorisme, le terme d'infraction terroriste sera lui aussi précisé dans le code pénal.

Al. 3 et 4

L'accès des autorités compétentes au CIR se fait selon un processus en deux étapes. Dans un premier temps, l'autorité en question peut uniquement savoir si des données relatives à une personne donnée figurent ou non dans les systèmes concernés. Si une recherche dans le CIR révèle qu'un des systèmes d'information Schengen-Dublin susmentionnés contient des données sur la personne concernée, le CIR affiche aux autorités visées à l'al. 2 la référence correspondante à l'EES, au VIS, à ETIAS ou à Eurodac.

Dans un deuxième temps, l'autorité doit demander l'accès aux données concernées en passant par la Centrale d'engagement de fedpol. Si elle renonce à demander un tel accès, malgré une référence, elle doit motiver par écrit sa décision ; les motifs sont consignés dans un fichier national traçable.

54 FF **2019** 4541
55 RS **312.0**

Section 3 Portail européen de recherche (ESP)

Art. 110e

L'ESP est conçu de manière à permettre la consultation simultanée et parallèle de tous les systèmes d'information Schengen-Dublin, des bases de données d'Interpol et des données Europol pertinents. Cette interface unique permettra la consultation instantanée des informations nécessaires dans les différents systèmes d'information. Elle respectera pleinement les droits d'accès et les exigences en matière de protection des données.

Après saisie des données d'identité, des données du document de voyage ou des données biométriques à caractère personnel, l'ESP permettra d'effectuer des recherches simultanément dans l'EES, le VIS, ETIAS, Eurodac, le SIS, le système d'information sur les documents volés et perdus d'Interpol (ASF-SLTD), la base de données d'Interpol sur les documents de voyage associés aux notices (TDAWN) et les données figurant dans Europol (art. 6 et 7 des règlements de l'UE sur l'interopérabilité). ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8.1).

Une recherche par l'ESP est lancée dans les cas suivants:

– des données sont entrées dans l'une des bases de données susmentionnées;
– des vérifications aux frontières extérieures de Schengen ou des contrôles d'identité sont effectués.

Une recherche peut également être lancée pour vérifier la légalité du séjour en Suisse de ressortissants d'États tiers.

Toutefois, la recherche au moyen de l'ESP n'est possible que pour les autorités autorisées à accéder à l'une des bases de données susmentionnées (art. 7 des règlements de l'UE sur l'interopérabilité). Afin de permettre l'utilisation de l'ESP, l'agence eu-LISA crée des catégories de profils d'utilisateurs de l'ESP qui tiennent compte des droits d'accès (art. 8 des règlements de l'UE sur l'interopérabilité).

Les utilisateurs voient s'afficher uniquement les données des systèmes auxquels ils ont accès et les liens visés aux art. 30 à 33 des règlements de l'UE sur l'interopérabilité. Aucune information n'est fournie sur les données auxquelles l'utilisateur n'est pas autorisé à accéder (art. 9 des règlements de l'UE sur l'interopérabilité).

Chaque État Schengen tient des journaux sur les consultations effectuées dans l'ESP par les autorités compétentes ou plus précisément par leur personnel.

Les interfaces nationales avec les différents systèmes d'information seront maintenues afin de disposer, si besoin est, d'autres solutions techniques.

Section 4 Détecteur d'identités multiples (MID)

Art. 110f Contenu du détecteur d'identités multiples

Le MID est à la fois un détecteur et une nouvelle base de données à laquelle certaines autorités ont accès. Cette base de données contient des dossiers de confirmation d'identité visés à l'art. 34 des règlements de l'UE sur l'interopérabilité. Les résultats des recherches sont enregistrés aussi longtemps que les données liées sont stockées dans au moins deux des systèmes d'information Schengen-Dublin (art. 35 des règlements de l'UE sur l'interopérabilité).

Al. 1

L'al. 1 définit les objectifs du MID, à savoir faciliter les contrôles d'identité et lutter contre la fraude identitaire.

Al. 2

L'al. 2 précise quand une détection d'identités multiples est automatiquement lancée conformément aux règlements de l'UE. Une recherche est automatiquement lancée dans le CIR et le SIS chaque fois qu'un dossier individuel est créé ou mis à jour dans l'EES, le VIS ou ETIAS, ou qu'un signalement est créé ou mis à jour dans le SIS. ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8.1).

Al. 3

L'al. 3 précise comment se déroule l'examen des identités multiples dans le cadre de l'interopérabilité des divers systèmes d'information Schengen. Le CIR, ETIAS, le VIS, l'EES (et, par la suite, Eurodac) ainsi que le SIS utilisent le sBMS (art. 110) et l'ESP (art. 110*e*) lors de la recherche d'identités multiples. Le sBMS permet d'effectuer une comparaison biométrique (art. 27, par. 2, des règlements de l'UE sur l'interopérabilité). L'ESP, quant à lui, permet d'effectuer une recherche à l'aide des données d'identité ou des données du document de voyage (art. 27, par. 3 et 4, des règlements sur l'interopérabilité). Cet examen a lieu lors de la création ou de la modification de dossiers des divers systèmes (cf. art. 110*f*, al. 2).

Al. 4

L'al. 4 précise les conditions pour la création d'un dossier de confirmation d'identité dans le MID conformément à l'art. 34 des règlements de l'UE sur l'interopérabilité. Un tel dossier est établi lorsqu'une recherche d'identités multiples révèle des liens entre des données de divers systèmes qui correspondent à la même personne et sont susceptibles de lui appartenir. Ces liens indiquent notamment les cas d'identités multiples légales ou frauduleuses. Le MID contient également une référence aux systèmes d'information concernés, sous la forme d'un numéro d'identification unique qui permet d'extraire des systèmes les données liées. Enfin, la date de création du lien, sa mise à jour, ainsi que l'autorité responsable de la vérification des liens sont mentionnés.

Art. 110g Vérification manuelle de différentes identités dans le MID

Al. 1

Une vérification manuelle doit avoir lieu à chaque fois que des correspondances entre des données de divers systèmes apparaissent et que les identités ne sont pas les mêmes ni similaires (liens jaunes, art. 28, par. 4, des règlements de l'UE sur l'interopérabilité). Afin de procéder à la vérification manuelle des données, les autorités chargées de la vérification (art. 110*c*) peuvent accéder au MID. Les autorités compétentes sont identiques à celles pouvant accéder au CIR pour détecter d'éventuelles identités multiples. Il est dès lors renvoyé à l'art. 110*c*, al. 1, qui désigne les autorités disposant de cet accès au CIR.

Al. 2

Cet alinéa précise quelle autorité est chargée de vérifier les liens jaunes dans le MID. Il s'agit en principe de l'autorité qui a lancé une recherche en créant un dossier ou en mettant à jour des données dans le C-VIS, l'EES, ou ETIAS (après l'approbation de la reprise de ce développement). Cependant, dans tous les cas où apparaît un lien avec un signalement de nature policière, le bureau SIRENE de fedpol est compétent.

Afin de soutenir la vérification manuelle des liens MID, il est prévu de créer un service central d'expertise (*zentrale MID-Expertenstelle*, MES). Ce service se composera de collaborateurs d'offices fédéraux habilités à vérifier des liens. L'objectif est que le MES puisse soutenir les autorités lorsqu'une affaire est particulièrement complexe ou qu'une autorité ne possède pas l'expertise nécessaire pour procéder à la vérification d'un lien.

Al. 3

Une vérification des différentes identités est lancée en présence de la personne concernée (art. 29 du règlement IOP Frontières), notamment lors du contrôle frontalier ou en cas de liens à vérifier sur le territoire suisse. Si des liens sont établis lors de la demande d'autorisation de voyage ETIAS, ce contrôle peut s'effectuer en l'absence de la personne.

Al. 4

Si une identité multiple frauduleuse (lien rouge, art. 32 des règlements de l'UE sur l'interopérabilité) est détectée ou si une personne figure de manière justifiée dans plusieurs systèmes d'information Schengen (lien blanc, art. 33 des règlements de l'UE sur l'interopérabilité), la personne concernée doit en être informée. L'autorité chargée de la vérification manuelle transmet cette information au moyen d'un formulaire. Par ailleurs, en cas d'établissement d'un lien rouge, le MID informe de manière automatisée les autorités responsables des données liées (art. 32, par. 6, des règlements de l'UE sur l'interopérabilité).

Section 5 Communication de données et responsabilité en matière de traitement de données

Art. 110h Communication de données du sBMS, du CIR et du MID

En principe, les données des composants d'interopérabilité ne peuvent être communiqués à des pays tiers, des organisations internationales ou des entités privées. Cependant, les règles de communication des données prévues pour chaque système restent valables (art. 50 des règlements sur l'interopérabilité). Celles-ci figurent dans l'article général 111*d* et dans les articles 103*d* et 108*f*[56], qui réglementent la communication des données des systèmes d'information EES et ETIAS. Les données de ces systèmes peuvent être transmises en tout temps conformément aux dispositions en vigueur ou à venir. Ces dispositions prévoient que les données des différents systèmes, y compris le contenu qui s'y rapporte dans le CIR, peuvent être communiquées dans certains cas.

Art. 110i Responsabilité en matière de traitement de données dans le sBMS, le CIR et le MID

Cette disposition renvoie à l'art. 40 des deux règlements de l'UE sur l'interopérabilité pour ce qui a trait à la responsabilité du traitement des données des trois composants d'interopérabilité que sont le sBMS, le CIR et le MID (cf. ch. 3.2, Protection des données).

Chapitre 14c Protection des données dans le cadre des accords d'association à Schengen

Le chapitre 14*b* devient le chapitre 14*c*, afin que toutes les dispositions concernant la protection des données dans le cadre des accords d'association à Schengen figurent après le nouveau chapitre 14*b* consacré à l'interopérabilité.

Aucune modification matérielle n'est apportée aux dispositions de ce chapitre.

L'art. 111*c*, al. 3, renvoie au nouvel art. 109*l*, ainsi qu'aux art. 111*a* et 111*d*. Il ne subit aucune modification matérielle.

L'art. 111*d*, al. 5, devient le nouvel art. 109*l*.

Le droit d'accès prévu à l'actuel art. 111*f* fait notamment référence à la LPD et aux lois cantonales sur la protection des données. Cette disposition vaut également pour les informations contenues dans les différents systèmes d'information Schengen-Dublin. Comme cet article reprend l'art. 8 LPD, le projet prévoit de l'abroger.

Le droit de rectification ou d'effacement des données est lui aussi régi par la LPD. Il en va de même du droit à l'information. Certains points concernant la protection des données relatifs aux divers systèmes d'information Schengen-Dublin et à l'interopérabilité sont ou seront concrétisés dans les ordonnances d'exécution. Ils ne sont donc pas mentionnés dans ce chapitre.

56 FF **2019** 4397

L'actuel chapitre 14*c*, consacré à Eurodac, est déplacé avant le chapitre consacré à l'interopérabilité. Il est donc abrogé à son emplacement actuel.

Art. 120d Traitement illicite de données personnelles dans les systèmes d'information

L'art. 45 des deux règlements de l'UE sur l'interopérabilité oblige les États Schengen à sanctionner l'utilisation abusive de données et le traitement ou l'échange d'informations illicite. Les sanctions prévues doivent être effectives, proportionnées et dissuasives. Des dispositions similaires figurent dans le règlement (CE) n° 767/2008 concernant le VIS (art. 36) et le règlement (UE) 2017/2226 sur l'EES (art. 48).

L'art. 120*d*, adapté dans le cadre du projet EES, doit donc à nouveau être modifié pour les besoins de l'interopérabilité.

Le projet ETIAS implique également une modification de la présente disposition. Ce projet est actuellement traité par le Parlement.

Tout d'abord, le titre de la disposition est modifié, car certains systèmes sont des systèmes d'information Schengen-Dublin (CIR et MID), lesquels ne relèvent pas uniquement du SEM. Le VIS, l'EES et bientôt ETIAS sont quant à eux des systèmes d'information Schengen-Dublin qui relèvent du SEM.

L'al. 1, qui a été ajouté dans le cadre du projet EES et qui n'est pas encore entré en vigueur, est adapté au présent projet et déplacé à l'art. 101, al. 2. Il ne subit aucune modification matérielle.

Par conséquent, l'art. 120*d* (état: adoption du projet EES par le Parlement) devra être adapté puisqu'il ne comportera plus d'alinéas.

L'al. 2, let. a, qui a été ajouté dans le cadre du projet EES et qui n'est pas encore entré en vigueur, figure désormais à la let. a (sans alinéa). Il prévoit des sanctions en cas de traitement illicite des données du C-VIS.

L'al. 2, let. b, qui a été ajouté dans le cadre du projet EES et qui n'est pas encore entré en vigueur, figure désormais à la let. b (sans alinéa). Il règle la même chose pour l'EES.

ETIAS sera également mentionné dans ces dispositions à l'avenir. Cet ajout fait cependant l'objet d'un projet à part, qui est cours d'examen au Parlement.

Une nouvelle let. c et une nouvelle let. d sont créées pour définir les règles applicables au CIR et au MID. Tout traitement des données contrevenant aux art 110*a à* 110*d*, 110*f* et 110*g* est passible, conformément à l'art. 106, al. 1, CP, d'une amende de 10 000 francs au plus lorsque des collaborateurs d'une autorité ayant compétence pour traiter des données personnelles les traitent délibérément de manière abusive.

La poursuite pénale impartit aux cantons conformément à l'actuel art. 120*e*.

Art. 122b, al. 2

Cf. commentaire relatif à l'art. 92*a*.

Art. 122c, al. 3, let. b

Cf. commentaire relatif à l'art. 92*a*.

Art. 126, al. 5

Cf. commentaire relatif à l'art. 102*e*.

7.2 Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA)

Art. 1, al. 2

Cf. commentaire relatif à l'art. 92*a* LEI.

Art. 15 Communication à des destinataires à l'étranger

Les art. 105 à 107 LEI sont remplacés par les art. 102*c* à 102*e* P-LEI. Le renvoi figurant à l'art. 15 LDEA doit être modifié en conséquence. Le renvoi aux art. 111*d*, al. 5, et 111*i* LEI doit également être remplacé par un renvoi aux nouveaux art. 109*k* et 109*l* P-LEI.

7.3 Loi du 14 mars 1958 sur la responsabilité (LRCF)

Titre du chap. Va

La responsabilité des dommages que cause une personne au service de la Confédération ou d'un canton lorsqu'elle traite sans droit des données doit être étendue à tous les systèmes d'information Schengen-Dublin et à leurs composants. Le titre du chapitre V*a* est adapté en conséquence.

Art. 19a

L'art. 19*a* réglemente la responsabilité découlant de l'exploitation du SIS. Il prévoit que la Confédération répond du dommage causé sans droit à un tiers lors de l'exploitation du SIS par une personne au service de la Confédération ou d'un canton. L'al. 2 ajoute que lorsque la Confédération répare le dommage, elle peut engager une action récursoire contre le canton au service duquel travaille la personne qui a causé le dommage.

L'article doit être étendu à tous les systèmes d'information Schengen-Dublin et à leurs composants. En effet, les bases légales européennes sur le sujet prévoient elles aussi qu'une personne victime d'un dommage matériel ou immatériel causé par un

traitement illégal de données est en droit de réclamer des dommages-intérêts à l'État Schengen responsable du dommage. S'agissant de l'EES, la disposition concernant la responsabilité se trouve à l'art. 45 du règlement (UE) 2017/2226, s'agissant du VIS, à l'art. 33 du règlement (CE) n° 767/2008, s'agissant d'ETIAS, à l'art. 63 du règlement (UE) 2018/1240, s'agissant d'Eurodac, à l'art. 37 du règlement (UE) n° 603/2013 et s'agissant des composants centraux, à l'art. 46 des règlements de l'UE sur l'interopérabilité.

Par conséquent, l'EES (let. b), le VIS (let. c), le CIR (let. d), l'ESP (let. e), le MID (let. f) et Eurodac (let. g) sont intégrés dans la disposition. ETIAS ne peut pas encore y être mentionné car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8.1).

Une petite adaptation formelle est par ailleurs apportée à la disposition, par souci de clarté : le terme « exploitation » est remplacé par « exploitation et utilisation ». La version française de l'art. 19*b* utilise déjà le terme « utilisation ».

Art. 19b

L'art. 19*b* comporte désormais deux alinéas. La formulation « d'un des systèmes d'information Schengen-Dublin ou d'un de leurs composants » remplace la référence au SIS à la let. a. La let. b, qui concerne actuellement un dommage en rapport avec un signalement dans le SIS, doit aussi être modifiée. Il doit y être question d'une façon plus générale de « traitement des données » pour couvrir tous les systèmes d'information Schengen-Dublin et leurs composants.

Les accords d'association à Schengen et Dublin doivent en outre être mentionnés dans une annexe. C'est ce que prévoit l'al. 2.

7.4 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)

Adaptation de la structure de l'acte

Plusieurs articles de la LSIP régissant les systèmes d'information Schengen-Dublin ou leurs composants doivent être complétés, raison pour laquelle plusieurs titres de section sont créés ou modifiés.

Art. 2

L'art. 2 énumère les systèmes d'information réglementés dans la LSIP. Comme indiqué au ch. 6.3.1, les composants centraux qui concernent le SIS doivent également être inscrits dans la LSIP. Ils sont donc ajoutés au présent article.

Une nouvelle subdivision sépare les systèmes d'information de police (let. a) et les systèmes d'information Schengen-Dublin et leurs composants (let. b).

À la let. a, le réseau de systèmes d'information de police (art. 9 à 14) est désormais mentionné au ch. 1, le système de recherches informatisées de police (art. 15) au

ch. 2, l'index national de police (art. 17) au ch. 3 et le système de gestion des affaires et des documents de fedpol (art. 18) au ch. 4.

À la let. b (systèmes d'information Schengen-Dublin et leurs composants), la partie nationale du système d'information Schengen (N-SIS; art. 16) est désormais mentionnée au ch. 1. Les composants centraux sBMS (régi à l'art. 16*a*), ESP (art. 16*b*) et MID (art. 16*c*) sont ajoutés aux ch. 2 à 4, dans l'ordre de leur mise en service prévue.

Art. 16a Service partagé d'établissement de correspondances biométriques (sBMS)

Le sBMS est lui aussi rattaché au SIS et doit donc être réglementé dans la LSIP, comme c'est le cas à l'art. 110 P-LEI. Même si les deux règlements de l'UE sur l'interopérabilité sont directement applicables, le sBMS est mentionné dans la LSIP par souci d'exhaustivité; il est ainsi plus facile d'y faire référence. Le sBMS n'est pas un fichier au sens de l'art. 3, let. g, LPD puisque les modèles biométriques ne permettent pas de rechercher les données par personne concernée.

Al. 1

Le sBMS contient les modèles biométriques générés à partir des images faciales et des empreintes digitales figurant dans le SIS et le CIR. Les données concernées du CIR proviennent de l'EES, du VIS et d'Eurodac. C'est ce que précise le présent alinéa.

Al. 2

L'al. 2 précise que le sBMS contient également une référence au système d'information Schengen-Dublin à partir duquel les modèles biométriques ont été générés ainsi qu'aux ensembles de données à proprement parler. Les données contenues sont séparées logiquement les unes des autres selon le système d'information dont elles sont issues.

Al. 3

Le sBMS permet d'effectuer des recherches simultanées au moyen de données biométriques. Si des ensembles de données sont saisis ou mis à jour, les données concernant les personnes enregistrées dans le CIR et dans le SIS sont automatiquement comparées.

Une suppression de données dans le CIR ou dans le SIS entraîne la suppression des données correspondantes dans le sBMS.

Art. 16b Portail de recherche européen (ESP)

L'ESP doit être réglementé non seulement dans la LEI (art. 110*e*) mais aussi dans la LSIP, puisqu'il englobe le SIS.

Al. 1

Comme indiqué à propos de l'art. 110*e* LEI, l'ESP permet, en une seule et même recherche , d'interroger simultanément tous les systèmes d'information Schengen-Dublin pertinents et leurs composants (SIS, EES, VIS, ETIAS, Eurodac et CIR), les bases de données d'Interpol ainsi que les données d'Europol. ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8).

Al. 2

Seules les autorités autorisées à accéder à au moins un des systèmes d'information Schengen-Dublin et leurs composants (SIS, EES, VIS, ETIAS, Eurodac et CIR), aux bases de données d'Interpol ou aux données d'Europol peuvent consulter l'ESP en ligne.

Al. 3

Les systèmes peuvent être interrogés au moyen des données d'identité, des données du document de voyage ou des données biométriques. La recherche peut porter sur des personnes ou des documents de voyage.

Al. 4

Le résultat de la recherche se limite aux systèmes d'information Schengen-Dublin, aux bases de données d'Interpol et aux données d'Europol pour lesquels les autorités concernées disposent d'un droit d'accès. Le système d'où proviennent les données ainsi que les liens existants s'affichent également.

L'eu-LISA doit définir dans un acte d'exécution, en collaboration avec les États Schengen, les champs de recherche à utiliser, les données spécifiques pouvant être consultées et les catégories de données pouvant s'afficher dans les résultats. Ces points seront précisés dans les ordonnances d'exécution.

Art. 16c Détecteur d'identités multiples (MID)

Le MID concernant aussi le SIS, il doit être réglementé tant dans la LEI (art. 110*f*) que dans la LSIP.

Al. 1

L'al. 1 définit la finalité du MID. Ce système sert à vérifier les identités et à lutter contre la fraude à l'identité.

Al. 2

Dans certaines circonstances, une recherche est automatiquement lancée afin de détecter les identités multiples dans le SIS et dans le CIR, par exemple lorsque des données sont saisies ou mises à jour dans le SIS, l'EES, ETIAS, le VIS et, dans l'avenir, Eurodac. ETIAS ne peut pas encore être mentionné dans le texte de loi car le Parlement n'a pas encore donné son feu vert à la reprise de ce développement (cf. ch. 8).

Al. 3

Le présent alinéa explique comment se déroule la vérification automatique des identités multiples. Afin de savoir si des données concernant une personne figurent déjà dans le SIS ou dans le CIR, les données saisies ou mises à jour sont comparées avec les modèles biométriques enregistrés dans le sBMS. De même, les données d'identité et les données du document de voyage sont comparées, via l'ESP, aux données alphanumériques existantes.

Si une ou plusieurs concordances en ressortent, le SIS et le CIR établissent un lien entre les données utilisées pour la recherche et les données ayant conduit à la concordance.

Al. 4

S'il existe un lien, un dossier de confirmation d'identité (cf. art. 34 des règlements de l'UE sur l'interopérabilité) est créé. Il contient les informations suivantes: le type de lien entre les données (en présence d'une concordance), la référence aux systèmes d'information Schengen-Dublin où sont enregistrées les données liées, un numéro d'identification unique permettant d'extraire des systèmes d'information Schengen-Dublin correspondants les données liées, l'autorité responsable de la vérification manuelle des différentes identités et la date de création ou de mise à jour du lien.

Art. 16d Vérification manuelle des liens dans le MID

Cet article désigne les autorités habilitées à procéder aux vérifications manuelles en cas de lien entre les systèmes d'information Schengen-Dublin (cf. art. 110, al. 1, P-LEI).

Al. 1

Les droits d'accès servent à la vérification manuelle des liens jaunes.

Al. 2

L'autorité qui saisit ou met à jour des données dans un système d'information Schengen-Dublin doit effectuer une vérification manuelle.

Si un lien concerne un signalement dans le SIS (sauf s'il s'agit d'un refus d'entrée), c'est le bureau SIRENE qui procède à la vérification manuelle. Si la vérification concerne l'EES, c'est l'AFD ou la police cantonale. Si le lien concerne le C-VIS, c'est le SEM ou d'autres autorités chargées des visas. Enfin, s'il concerne ETIAS, c'est le SEM.

L'autorité chargée de la vérification manuelle se voit octroyer un accès aux données dont elle a besoin pour contrôler l'identité. Il s'agit d'une part des données liées contenues dans le dossier de confirmation d'identité concerné et d'autre part des données d'identité liées dans le CIR et dans le VIS. Le contrôle des différentes identités doit être immédiat. Il faut alors classer le lien comme vert (les données d'identité des données liées n'appartiennent pas à la même personne), rouge (il y a identités multiples illicites ou fraude à l'identité) ou blanc (il s'agit de la même personne) et compléter le dossier de confirmation d'identité. Chaque lien doit être vérifié.

Al. 4

Si la vérification manuelle indique des identités multiples illicites (lien rouge) ou qu'une personne figure dans plusieurs systèmes d'information Schengen-Dublin (lien blanc), la personne concernée doit en être informée au moyen d'un formulaire type. L'autorité peut ne pas l'informer si cette information irait à l'encontre d'un signalement dans le SIS ou, si nécessaire, pour protéger la sécurité et l'ordre publics, pour prévenir la criminalité ou pour garantir qu'aucune enquête nationale ne sera compromise.

Le MID informe automatiquement les autorités chargées des données d'un lien rouge.

La vérification manuelle d'identités multiples doit, dans la mesure du possible, se faire en présence de la personne concernée, par exemple lors d'un contrôle à l'entrée en Suisse en tant que premier État Schengen.

Art. 16e Communication de données du sBMS, du CIR et du MID

Le présent article prévoit que les données personnelles enregistrées ou traitées dans les composants de l'interopérabilité ou auxquelles il est possible d'accéder via ces composants ne peuvent en principe être transmises à des États tiers, des organisations internationales ou des services privés ni mises à la disposition de ceux-ci. . Les prescriptions prévues pour chacun des systèmes relatives à la communication des données continuent de s'appliquer.

Art. 16f Responsabilité en matière de traitement des données dans le sBMS, le CIR et le MID

La responsabilité du traitement des données doit elle aussi être réglementée. Elle se fonde sur l'art. 40 des règlements de l'UE sur l'interopérabilité.

8 Besoins de coordination

8.1 Coordination avec le projet d'arrêté fédéral ETIAS

Les références à l'interopérabilité figurant aux art. 110*a*, al. 1, 110*c*, 110*e*, al. 1, et 110*f*, al. 2, LEI devraient mentionner le système ETIAS. Toutefois, le Parlement n'adoptera vraisemblablement pas le projet de reprise du règlement sur ETIAS[57] avant la session d'automne 2020, et il n'est pas possible de mentionner ETIAS avant cette date. Après le vote final, ces articles pourront être modifiés pour faire référence à ETIAS. En outre, l'art. 19*a*, al. 1bis, LRCF, qui régit actuellement la responsabilité en matière de systèmes de l'UE, devra également mentionner ETIAS. Le système ETIAS devra être mentionné dans les art. 16*b*, al. 1, et 16*c*, al. 2, LSIP, qui sont consacrés à l'ESP et au MID.

Le Département fédéral de justice et police (DFJP) proposera ces adaptations dans le cadre des débats parlementaires sur l'interopérabilité.

Quelques dispositions du projet ETIAS, qui sont actuellement soumis au Parlement, devront également être modifiées en raison de l'interopérabilité. Il s'agit des articles 5 al. 1, let. a^{bis}, 108*a*, 108*f* et 120*d* LEI. Ils devront être modifiés comme suit:

La note de bas de page de l'art. 5, al. 1, let. a^{bis}, LEI du projet ETIAS devra être mise à jour, étant donné que le règlement (UE) 2018/1240 sera modifié par le règlement IOP Frontières.

La section consacrée à la réglementation relative à ETIAS (art. 108*a* à 108*g*) doit être adaptée à la nouvelle structure prévue dans le présent projet (cf. ch. 7, commentaires sur le chap. 14*a*). Le titre de la section précédant l'art. 108*a* et tous les titres de section qui suivent sont renumérotés en conséquence.

L'art. 108*a* LEI règle les données que contient ETIAS. Certaines d'entre elles seront désormais stockées dans le CIR. Les données d'identité et les données du document de voyage (art. 108*a*, al. 1, let. a, de la version du projet ETIAS) seront enregistrées dans le CIR. Les informations relatives aux demandes d'autorisation de voyage ETIAS acceptées ou rejetées ainsi que les données figurant sur la liste de surveillance seront exclues des données à saisir dans le CIR; elles continueront donc de n'être enregistrées que dans ETIAS.

L'art. 108*f* LEI de la version du projet ETIAS actuellement soumis au parlement devra également être modifié. Cet article règle la communication des données ETIAS. Un nouvel al. 3 viendra s'y ajouter. Comme le CIR fera désormais partie d'ETIAS, les dispositions relatives à la communication des données ETIAS s'appliqueront également aux données ETIAS enregistrées dans le CIR (données d'identité, données du document de voyage et données biométriques). S'agissant de

57 Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE sur la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (Développement de l'acquis de Schengen), FF *2020* 2849.

la communication des données ETIAS enregistrées dans le CIR, un nouvel al. 3 renverra à l'art. 110*h*, lequel renvoie à son tour à l'art. 40 des deux règlements de l'UE sur l'interopérabilité. Cette disposition est analogue à celle applicable à l'EES (art. 103*d*, al. 3, LEI du présent projet).

Enfin, le contenu de l'art. 120*d*, al. 2, LEI tel qu'actuellement soumis au Parlement dans le cadre d'ETIAS devra être intégrée dans la formulation de l'art. 120*d* du présent projet.

En conséquence, ces articles devront encore être adaptés après le vote final au sujet du projet ETIAS.

8.2 Coordination avec la modification de la LEI du 14 décembre 2018 relative à la mise en œuvre des normes procédurales et des systèmes d'information

Un éventuel besoin de coordination du présent projet avec l'art. 111 LEI (Système d'information sur les documents de voyage) doit être assuré. Cette disposition doit être abrogée dans le cadre du projet « Normes procédurales et systèmes d'information »[58]. Toutefois, l'abrogation de cet article n'a pas encore été mise en vigueur, contrairement à toutes les autres dispositions du projet. En effet, le SEM dépend encore de l'actuel système d'établissement de documents de voyage pendant une période transitoire. Si l'art. 111 LEI n'est pas encore abrogé à l'entrée en vigueur de l'arrêté fédéral concernant l'interopérabilité, sa numérotation devra être modifiée étant donné qu'il n'a aucune raison de figurer dans la nouvelle section consacrée à la communication de données et à la responsabilité concernant leur traitement.

8.3 Coordination avec le projet d'arrêté fédéral SIS

L'interopérabilité doit être coordonnée avec la révision en cours de la LEI et de la LSIP prévue dans le cadre du projet relatif au SIS[59]. Le Parlement examine actuellement le projet d'arrêté fédéral concernant le SIS. Ce dernier devrait normalement être adopté par le Parlement soit lors de la session d'automne, soit lors de celle d'hiver 2020.

Que cette modification de la LSIP entre en vigueur après ou en même temps que l'arrêté fédéral relatif au SIS, l'art. 16, al. 1, 1re phrase, LSIP doit être adapté doivent être adaptés la 1re phrase de l'al. 1 conformément à la version relative à

58 RO **2019** 1413, FF **2018** 1673

59 Message du 6 mars 2020 relatif à l'approbation et à la mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases légales concernant l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) (développements de l'acquis de Schengen) et à la modification de la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile, FF **2020** 3465, objet Curia nº 20.025

l'interopérabilité. L'al. 2, let. b du présent projet devra être reprise comme let. c dans la version relatif au SIS.

Enfin, le règlement (UE) 2018/1861 étant modifié par le règlement « IOP Police », la note de bas de page de l'art. 68*a*, al. 2, LEI doit être modifiée en conséquence.

8.4 Coordination avec le projet d'arrêté fédéral EES

Le 21 juin 2019, le Parlement a adopté l'arrêté fédéral relatif à l'EES[60]. Le projet qui s'y rapporte prévoit de modifier la LEI en y ajoutant de nouvelles dispositions relatives au système d'information EES.

Les modifications de la LEI prévues par le présent projet se fondent sur les dispositions de l'arrêté fédéral relatif à l'EES, étant donné que celui-ci a déjà été approuvé.

L'interopérabilité reprend les dispositions de l'arrêté relatif à l'EES, tel qu'adopté par le Parlement, tout en y ajoutant des compléments indispensables à l'interopérabilité (Section 2 Système d'entrée et de sortie (EES) et contrôle automatisé à la frontière). Si l'arrêté fédéral sur l'interopérabilité entre en vigueur en même temps que l'arrêté fédéral relatif à l'EES, ce sont les dispositions de l'arrêté fédéral sur l'interopérabilité qui devraient valoir.

9 Conséquences

9.1 Conséquences financières et conséquences sur l'état du personnel pour la Confédération

Pour la Confédération, le projet aura des conséquences du point de vue des finances et du personnel aussi bien durant la phase de projet qu'à partir de la mise en service prévue de la plateforme d'interopérabilité. L'interopérabilité entraînera des avantages considérables tant pour la Confédération que pour les cantons.

9.1.1 Conséquences financières et conséquences sur l'état du personnel: phase de projet

Pour la Confédération, le coût total des projets d'interopérabilité est estimé à 21 millions de francs pour toute la période allant de 2020 à 2025.

Coût des projets d'interopérabilité (en millions de francs)	Total	2020	2021	2022	2023	2024	2025

60 Arrêté fédéral concernant l'approbation et la mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise des bases juridiques en vue de la création et de l'utilisation du système d'entrée et de sortie (EES) (règlements [UE] 2017/2226 et 2017/2225) ; (développements de l'acquis de Schengen) et modification de la loi sur les étrangers et l'intégration (LEI), FF **2019** 4573

fedpol	**11,3**	2,9	3,1	1,4	1,5	1,2	1,2
SEM	**7,7**	2,1	2,2	2,4	1,0		
Développement du projet (au SEM)	**2,0**					1,0	1,0
Total	**21,0**	**5,0**	**5,3**	**3,8**	**2,5**	**2,2**	**2,2**

Les projets de fedpol et du SEM relèvent d'un crédit d'engagement pour le développement de l'acquis de Schengen et Dublin, qui fait partie d'un programme géré par le Secrétariat général du DFJP (SG-DFJP). Ce programme est mené en tant que projet informatique clé. L'arrêté fédéral relatif au crédit d'engagement[61] a été approuvé par le Conseil national le 21 décembre 2019 et par le Conseil des États le 11 juin 2020. Le besoin de financement total de ces projets s'élève à 14,1 millions de francs pour les années 2020 à 2022. Sur cette somme, 9,8 millions proviennent de la première tranche du crédit d'engagement; ils sont couverts par les ressources centralisées destinées aux TIC allouées par la Confédération et par des ressources propres au DFJP. À partir de 2023, le financement de ces projets devrait être assuré dès que la deuxième tranche du crédit d'engagement aura été libérée.

La reprise et la mise en œuvre de l'interopérabilité entraîneront des modifications techniques. Des composants techniques supplémentaires au niveau national garantiront le raccordement des systèmes suisses à l'ESP. Un client MID national est également indispensable à la vérification des liens MID (cf. ch. 5.1). Ces composants seront fournis par le Centre de services informatiques du DFJP (CSI-DFJP). Les coûts de développement sont compris dans les coûts de projet présentés plus haut. Les exigences techniques sont spécifiées par l'agence eu-LISA. Il faut également s'attendre à ce que les composants nationaux doivent être adaptés à l'évolution des composants de l'UE. Ces adaptations seront réalisées après l'entrée en service, prévue en 2023, dans le cadre des développements du projet concernant l'interopérabilité au SEM. Pour ce dernier projet, des coûts de 1 million de francs sont prévus pour 2024 et 2025 respectivement.

À fedpol, les charges de personnel qu'entraînera la mise en œuvre de la phase de projet de 2020 à 2023 devraient s'élever à 2800 jours-personnes. Le SEM, pour sa part, prévoit 3960 jours-personnes. Les ressources correspondantes en personnel seront compensées à l'interne.

Pour l'AFD, l'augmentation des charges ayant une incidence financière concernant la gestion du projet et les coûts de développement relatifs à la modification des solutions mobiles et fixes de contrôle à la frontière se situeront probablement au niveau inférieur d'une fourchette qui va de 1 à 9 millions de francs. Selon les informations dont on dispose aujourd'hui, ces coûts font partie du programme DaziT de

61 Arrêté fédéral du 11 juin 2020 allouant un crédit d'engagement pour le développement de l'acquis de Schengen et Dublin, FF **2020** 6267.

l'AFD. Les obligations financières qui en résultent seront imputées sur le crédit d'ensemble de ce programme.

9.1.2 Conséquences financières et conséquences sur l'état du personnel: mise en service

Coûts d'exploitation

Des coûts d'exploitation de 0,2 million de francs devront probablement être engagés pour 2023 et un budget annuel d'environ 2 millions de francs sera nécessaire à partir de 2024 pour deux composants d'interopérabilité nationaux. Ce budget est nécessaire pour garantir l'extension de l'interopérabilité aux systèmes nationaux et permettra la vérification des liens MID. Au niveau national, l'interopérabilité ne constitue pas un projet purement organisationnel, mais implique également la création et l'exploitation de composants techniques nationaux. À l'heure de la rédaction du message relatif au crédit d'engagement[62] pour le développement de l'acquis de Schengen et Dublin, l'ampleur de sa mise en œuvre n'était pas encore connue, l'UE n'ayant pas encore fourni les informations correspondantes. Les coûts de fonctionnement récurrents (annuels) induits par la plateforme d'interopérabilité à partir de sa mise en service sont désormais estimés à quelque 2 millions de francs par an, et non à 0,2 million comme indiqué dans le message relatif au crédit d'engagement. Cette estimation est le fruit d'une comparaison avec le projet EES, dans le cadre duquel le CSI-DFJP devra également fournir et exploiter deux composants nationaux, pour des coûts prévus de fonctionnement similaires. Les ressources financières nécessaires au fonctionnement du système seront précisées lors de la phase conceptuelle du projet; elles donneront lieu à une proposition couvrant le montant requis lors de l'élaboration du budget 2024.

Conséquences de la vérification des liens MID sur l'état du personnel

Les débuts de l'interopérabilité, en 2023, entraîneront une augmentation du nombre de résultats positifs. Ceux-ci devront ensuite faire l'objet de clarifications manuelles. Les liens MID qui présentent des données divergentes (liens jaunes) devront toujours être vérifiés un à un. À cet égard, les deux règlements de l'UE sur l'interopérabilité prévoient que la vérification individuelle des liens MID est effectuée par l'autorité qui saisit ou met à jour les données ayant conduit à un lien MID. En Suisse, cette tâche incombe à fedpol, au SEM, à l'AFD, aux représentations suisses à l'étranger du Département fédéral des affaires étrangères (DFAE) ainsi qu'aux polices cantonales et aux autorités de migration. Un lien jaune MID est par exemple créé quand le ressortissant d'un État tiers ayant fait l'objet d'un signalement aux fins de non-admission (interdiction d'entrée) dans le SIS dépose une demande de visa Schengen en faisant usage d'un faux passeport. Ses empreintes digitales sont alors identiques dans le SIS et le VIS, mais pas ses données d'identité. Le lien MID correspondant donne donc lieu à une vérification individuelle. Les

62 Message du 4 septembre 2019 relatif à un crédit d'engagement pour le développement de l'acquis de Schengen et Dublin, FF **2019** 5881.

clarifications supplémentaires qui s'ensuivent pour établir avec certitude l'identité de la personne concernée sont indispensables. D'une part, cette démarche facilite la mobilité des personnes qui voyagent en toute légalité et, d'autre part, la vérification manuelle permet de détecter et de prévenir les usurpations d'identité. Pour accomplir cette nouvelle tâche, les autorités compétentes auront besoin de personnel supplémentaire. Selon les informations à disposition, on estime que les autorités suisses devront vérifier individuellement chaque année quelque 10 000 liens jaunes du MID. Quelque 60 % de ces liens concerneront probablement des données du SIS. Ces composants seront vérifiés par le bureau SIRENE de fedpol, pour le compte des cantons ou d'autres autorités. Les 40 % restants seront traités par le SEM, l'AFD, le DFAE, les polices cantonales ou les autorités cantonales de migration.

L'évaluation de plusieurs options organisationnelles a montré que les autorités compétentes dans le domaine des migrations devraient être soutenues, pour la vérification des liens MID, par un service d'experts du MID (MES) géré et financé par la Confédération. Le MES devrait être rattaché au SEM. Cet organe permettra aux autorités compétentes d'obtenir du soutien dans les cas complexes, ce qui évitera une charge supplémentaire sur leurs activités quotidiennes. Le MES apportera aussi son soutien, par exemple, à des autorités qui, à l'instar des ambassades suisses à l'étranger, n'ont que très rarement besoin de vérifier un lien MID et ne disposent donc pas du savoir-faire requis. Cette centralisation limitée permettra de profiter d'effets de synergie et de réaliser dès lors des économies. En tant que centre de compétence, le MES produira aussi des effets de synergie qualitatifs en regroupant des connaissances de différents domaines, ce qui permettra d'améliorer la qualité des vérifications et de raccourcir les canaux de communication. Le MES devrait employer du personnel issu de différents services fédéraux. Son organisation et sa composition exactes seront définies lors de la phase conceptuelle. Le MES ne pourra cependant pas vérifier des liens de manière autonome: il ne sera habilité qu'à restituer à l'autorité compétente les résultats obtenus, après vérification d'un lien MID. Cette autorité jugera ensuite si les divergences sont légitimes ou s'il y a eu usurpation d'identité. Le bureau SIRENE suisse devra toujours vérifier les liens MID contenant des données SIS. Les besoins supplémentaires en personnel pour le MES sont indiqués dans le tableau des dépenses supplémentaires en matière de personnel présenté plus bas.

Quand l'interopérabilité sera opérationnelle en 2023, du personnel formé devra être disponible. D'ici au milieu de l'année 2021, le DFJP évaluera le nombre de postes supplémentaires qui seront nécessaires à partir de 2023, en tenant compte du réexamen des tâches en cours au DFJP et des mutations internes correspondantes. Tout besoin de ressources supplémentaires sera soumis au Parlement dans le cadre du message concernant le budget 2022 assorti d'un plan intégré des tâches et des finances.

Selon l'estimation préliminaire du DFJP, les dépenses supplémentaires en matière de personnel décrites en détail dans les prochains sous-chapitres se répartissent comme suit:

Besoins supplémentaires en matière de personnel (estimation)

	à partir de 2023
Équivalents plein temps (EPT)	
fedpol	11
SEM	6
AFD	1
DFAE	0,9
Cantons (polices cantonales et services de migration)	1,1
Total	**20**

Conséquences sur l'état du personnel pour fedpol

Le bureau SIRENE est tenu de vérifier les liens MID qui se rapportent à des signalements SIS. Il est ensuite parfois nécessaire de procéder à des clarifications et de mener des recherches approfondies tant en Suisse qu'auprès d'autres États Schengen. Aujourd'hui, le développement du SIS impose déjà au bureau SIRENE un délai de traitement ferme de 12 heures et crée de nouvelles catégories de signalements. Pour les échanges d'informations, le bureau SIRENE devra être fonctionnel 24 heures sur 24 et 7 jours sur 7. Il devra donc recourir à des équipes, ce qui impliquera une augmentation de ses effectifs la nuit, le week-end et les jours fériés.

La vérification des liens MID en vue de détecter les signalements SIS inclura aussi un contrôle de concordance des données biométriques. La comparaison des données biométriques sera effectuée 24 heures sur 24 et 7 jours sur 7 par des équipes rattachées à la Division Identification biométrique.

L'interopérabilité automatisera la comparaison des données policières avec les données d'autres systèmes d'information de l'UE. Ainsi, les autorités policières disposeront de plus en plus souvent d'informations policières significatives susceptibles de déboucher sur des enquêtes. L'interopérabilité augmentera donc aussi les tâches de coordination et de préparation de la Police judiciaire fédérale.

Toutes les tâches décrites ci-dessus occasionneront, dans les différents domaines concernés, un surcroît de travail impossible à accomplir sans ressources supplémentaires. fedpol estime que le nombre total de collaborateurs supplémentaires dont il aura besoin à compter de la mise en œuvre de la plateforme d'interopérabilité se montera à 11 EPT.

Conséquences sur l'état du personnel pour le SEM

Au SEM, la vérification des liens MID incombera au Domaine de direction Immigration et intégration. En effet, c'est à cette unité organisationnelle que sont rattachées les autorités compétentes du SEM, définies conformément aux règlements de l'UE. La vérification des liens MID au SEM impliquera une charge supplémentaire totale de 5 EPT. Une partie de ces postes sera consacrée au MES, qui traitera les liens MID complexes relevant du domaine de la migration.

Les tâches de gestion et de soutien sont déjà incluses dans les 5 EPT. En outre, le SEM devra assumer des tâches liées à la responsabilité des applications et des produits concernant les composants techniques nationaux.

Les effectifs supplémentaires requis au SEM se monteront, en tout, à 6 EPT.

Conséquences sur l'état du personnel pour l'AFD

Le présent développement de l'acquis de Schengen aura pour l'AFD des conséquences du point de vue des finances, des procédures et du personnel. D'une part, les systèmes actuels devront être adaptés aux nouvelles interfaces. D'autre part, plusieurs nouveaux systèmes tels que l'ESP, obligatoire pour les contrôles aux frontières extérieures de Schengen, devront être mis en œuvre. De surcroît, il faudra encore tenir compte des éventuelles modifications que pourrait induire la création d'une plateforme de recherche nationale (cf. ch. 9.2.2).

L'ESP sera indispensable pour procéder au contrôle des personnes aux frontières extérieures de Schengen. Il entraînera des ajustements dans les processus opérationnels, en particulier pour la détection des identités multiples et des fausses identités. Actuellement, l'on peut estimer que les gains d'efficacité inhérents à toute automatisation accrue et les efforts de détection des fausses identités s'équilibreront plus ou moins. La vérification des liens MID, y compris les mesures ayant trait à la formation du personnel, imposera une faible charge supplémentaire à l'AFD et sera compensée à l'interne.

Conséquences sur l'état du personnel pour la Direction consulaire et les représentations suisses à l'étranger (DFAE)

La Direction consulaire du DFAE soutient les représentations à l'étranger dans la fourniture de services consulaires. Elle tient à leur disposition des outils de travail appropriés et coordonne la coopération avec les partenaires nationaux et internationaux. Chaque représentation à l'étranger sera responsable de la vérification des liens MID lorsque les données concernant une demande de visa traitée par elle débouchent sur un lien MID vers les données d'un autre système d'information de l'UE. Pour l'heure, on peut supposer que les charges supplémentaires en personnel de la Direction consulaire et des représentations étrangères pourront être compensées au sein même du département. Le soutien apporté par le MES déchargera les représentations à l'étranger dans les cas complexes nécessitant des clarifications poussées.

9.2 Conséquences pour les cantons

Les règlements de l'UE sur l'interopérabilité permettront également aux police cantonales et aux autorités de migration de disposer en permanence des informations les plus pertinentes. Les bénéfices attendus sont considérables, mais un certain surcroît de travail pour les cantons ne saurait être exclu.

9.2.1 Conséquences financières et conséquences sur l'état du personnel

L'interopérabilité permettra également aux police cantonales et aux autorités de migration de faire un usage plus efficace et mieux ciblé des informations à leur disposition. Le risque que des identités multiples restent non détectées sera réduit et le nombre de résultats positifs augmentera. Il est prévu que les polices cantonales et communales puissent accéder aux données du CIR pour identifier les personnes déjà présentes dans l'espace Schengen. Dans leur travail de prévention, d'enquête, de détection du terrorisme ou d'autres infractions pénales graves et de poursuites en la matière, les polices cantonales pourront également bénéficier de l'accès octroyé aux autorités pénales. Une recherche dans le CIR leur permettra de déterminer si l'un des systèmes d'information de l'UE comporte des données concernant une personne. En sa qualité de point d'accès central pour les requêtes de recherche des autorités de poursuite pénale dans les systèmes d'information non policiers, fedpol a la compétence, dans un deuxième temps, d'accorder l'accès aux données requises auxdites autorités. Déjà appliqué dans le cas du VIS, ce processus est également prévu pour l'EES.

L'utilisation de l'ESP sera obligatoire dans le cadre du contrôle aux frontières extérieures de l'espace Schengen. Outre l'AFD, les polices cantonales chargées du contrôle des frontières extérieures de Schengen seront également concernées par cette mesure, car elles vérifieront les liens MID qui concernent les données de l'EES. Cette nouvelle tâche se traduira par du travail supplémentaire. Dans les cas complexes qui nécessitent des clarifications poussées, le soutien apporté par le MES déchargera les polices cantonales et les autorités de migration.

La Confédération fournira un « client » (composant national) pour la vérification des liens MID. Son intégration dans les systèmes cantonaux relèvera des cantons. Le rattachement des systèmes de recherche nationaux à l'ESP nécessitera des interventions techniques sur les systèmes de recherche cantonaux. Ces modifications relèveront aussi de la responsabilité des cantons. D'autres interventions sont envisageables, mais à ce stade, on ne saurait les identifier de manière définitive. Les cantons seront associés aux groupes de travail à un stade précoce afin d'assurer une étroite coopération dans la mise en œuvre.

9.2.2 Plateforme de recherche nationale

L'interopérabilité au niveau de l'UE ainsi que la motion Eichenberger[63] ont aussi incité la Suisse à rendre les systèmes d'information cantonaux interopérables, non seulement entre eux mais également avec ceux de la Confédération. Distinct de la reprise des règlements de l'UE sur l'interopérabilité, le projet de plateforme de recherche nationale (PRN) est dirigé par les cantons. En principe, des derniers se chargent du maintien de la sécurité et de l'ordre publics sur leur territoire. Ce sont eux qui sont compétents au premier chef en matière policière. La Confédération assume aussi certaines tâches policières, mais dans des domaines spécifiques. Une

[63] Motion 18.3592, Échange de données de police au niveau national

PRN permettra d'exploiter des synergies entre les systèmes d'information nationaux et cantonaux et de présenter les résultats des recherches aux utilisateurs de manière plus claire et uniforme. Les avantages et la faisabilité d'une PRN étant clairement établis, un projet a été lancé dans le cadre de l'harmonisation des systèmes informatiques de police en Suisse (Centre de compétence pour la technique policière et informatique). Il devrait prévoir une centralisation de l'exploitation de la PRN, le stockage des données et l'exploitation des systèmes d'information étant appelés à rester du ressort de chacune des autorités concernées. Les droits d'accès des autorités resteraient identiques (cf. commentaire de l'art. 16*b*, al. 5, P-LSIP). Comme le projet de mise en œuvre technique de la PRN vient seulement d'être lancé, ses spécifications techniques sont encore trop vagues pour en déduire les implications législatives. La base légale de la PRN fera ultérieurement l'objet d'une proposition, dans le cadre d'un projet à part.

9.3 Conséquences dans d'autres domaines

Le projet ne devrait pas avoir de conséquences directes dans les domaines de l'économie, de la société et de l'environnement. L'interopérabilité augmentera le niveau de sécurité dans l'espace Schengen, avec des répercussions positive sur l'économie et la société.

10 Aspects juridiques

10.1 Constitutionnalité

Les échanges de notes entre la Suisse et l'UE concernant la reprise des règlements de l'UE sur l'interopérabilité se fondent sur l'art. 54, al. 1, Cst., qui prévoit que les affaires étrangères relèvent de la compétence de la Confédération. Le Conseil fédéral signe et ratifie les traités internationaux (art. 184, al. 2, Cst.) et l'Assemblée fédérale les approuve (art. 166, al. 2, Cst.), à l'exception de ceux dont la conclusion relève de la seule compétence du Conseil fédéral en vertu d'une loi ou d'un traité international. En l'occurrence, le Conseil fédéral ne peut invoquer cette compétence (cf. art. 7*a*, al. 1 et 2, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[64] et art. 24, al. 2, de la loi du 13 décembre 2002 sur le Parlement [LParl][65]). L'approbation des deux échanges de notes incombe donc à l'Assemblée fédérale.

10.2 Compatibilité avec les obligations internationales de la Suisse

En reprenant les deux développements de l'acquis de Schengen, la Suisse remplit ses obligations découlant de l'AAS. Elle contribue par ailleurs à l'utilisation uniforme des systèmes d'information Schengen et Dublin. La reprise des deux règlements

64 RS **172.010**
65 RS **171.10**

européens et les modifications légales qu'elle induit sont ainsi conformes aux obligations internationales de la Suisse.

10.3 Forme de l'acte à adopter

La reprise des deux règlements de l'UE ne représentant pas une adhésion de la Suisse à une organisation de sécurité collective ou à une communauté supranationale, le présent arrêté fédéral n'est pas soumis au référendum obligatoire visé à l'art. 140, al. 1, let. b, Cst.

En vertu de l'art. 141, al. 1, let. d, ch. 3, Cst., les traités internationaux sont soumis au référendum facultatif s'ils contiennent des dispositions importantes fixant des règles de droit ou si leur mise en œuvre exige l'adoption de lois fédérales. Sont réputées fixant des règles de droit les dispositions générales et abstraites d'application directe qui créent des obligations, confèrent des droits ou attribuent des compétences (art. 22, al. 4, LParl). Sont par ailleurs réputées importantes les dispositions qui, sur la base de l'art. 164, al. 1, Cst., devraient être édictées dans le droit interne sous la forme d'une loi fédérale.

Les présents règlements européens, repris par échange de notes, contiennent d'importantes dispositions fixant des règles de droit telles que les droits de consultation et d'accès à des systèmes d'information. Leur reprise requiert en outre des adaptations au niveau de la loi (cf. ch. 6.2). Le présent arrêté fédéral est donc soumis au référendum facultatif en vertu de l'art. 141, al. 1, let. d, ch. 3, Cst.

L'Assemblée fédérale approuve les traités internationaux sous la forme d'un arrêté fédéral lorsqu'ils sont soumis ou sujets à référendum (art. 24, al. 3, LParl).

En vertu de l'art. 141*a*, al. 2, Cst., lorsque l'arrêté portant approbation d'un traité international est sujet au référendum, l'Assemblée fédérale peut y intégrer les modifications de lois liées à la mise en œuvre du traité.

Les dispositions législatives proposées dans le projet servent à la mise en œuvre des bases juridiques de l'interopérabilité des systèmes d'information de l'UE et découlent directement des obligations qui y sont contenues. Le projet d'acte de mise en œuvre peut dès lors être intégré dans l'arrêté portant approbation.

10.4 Frein aux dépenses

Le projet n'implique pas de nouveaux crédits d'engagement ou plafonds de dépenses qui entraîneraient de nouvelles dépenses uniques de plus de 20 millions de francs. Il n'est donc pas soumis au frein aux dépenses (art. 159, al. 3, let. b, Cst.).

Liste des abréviations utilisées

AAD	Accord du 26 octobre 2004 entre la Confédération suisse et la Communauté européenne relatif aux critères et aux mécanismes permettant de déterminer l'État responsable de l'examen d'une demande d'asile introduite dans un État membre ou en Suisse, RS *0.142.392.68*
AAS	Accord du 26 octobre 2004 entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, RS *0.362.31*
AFD	Administration fédérale des douanes
ASM	Association des services cantonaux de migration
AsyLex	Organisation d'aide en ligne au droit d'asile suisse
Bureau SIRENE	Point de contact national pour toutes les recherches lancées via le SIS (SIRENE = *Supplementary Information Request at the National Entries*)
CIR	Répertoire commun de données d'identité
Commission LIBE	Commission des libertés civiles, de la justice et des affaires intérieures
COREPER	Comité des représentants permanents des États membres
CP	Code pénal, RS *311.0*
CSI-DFJP	Centre de services informatiques du DFJP
Cst.	Constitution fédérale, RS *101*
C-VIS	Système central d'information sur les visas
DFAE	Département fédéral des affaires étrangères
DFJP	Département fédéral de justice et police
ECRIS-TCN	Système européen d'information sur les casiers judiciaires de ressortissants d'États tiers
EES	Système d'entrée et de sortie
EPT	Équivalent plein temps
ESP	Portail de recherche européen
ETIAS	Système européen 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
Eurodac	Banque de données centrale de l'Union européenne

	contenant les empreintes digitales de personnes qui ont déposé une demande d'asile dans un État Dublin et ont été appréhendées lors de leur entrée irrégulière
Europol	Office européen de police
fedpol	Office fédéral de la police
Interpol	Organisation internationale de police criminelle (*International Criminal Police Organization*)
LDEA	Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile, RS *142.51*
LEI	Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration, RS *142.20*
LParl	Loi du 13 décembre 2002 sur le Parlement, RS *171.10*
LPD	Loi fédérale du 19 juin 1992 sur la protection des données, RS *235.1*
LPDS	Loi du 28 septembre 2018 sur la protection des données, RS *235.3*
LRCF	Loi du 14 mars 1958 sur la responsabilité, RS *170.32*
LSIP	Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération, RS *361*
MES	Service central d'expertise
N-SIS	Partie nationale du Système d'information Schengen
NUI	Interface nationale entre les systèmes nationaux des États Schengen et les composants centraux de l'UE (*National Uniform Interface*)
ORBIS	Système national d'information sur les visas
OSAR	Organisation suisse d'aide aux réfugiés
PFPDT	Préposé fédéral à la protection des données et à la transparence
PRN	Plateforme de recherche nationale
Règlement IOP Frontières	Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, version du JO L 135 du 22.5.2019, p. 27
Règlement IOP Police	Règlement (UE) 2019/818 du Parlement européen et

	du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816, version du JO L 135 du 22.5.2019, p. 85
Règlements de l'UE sur l'interopérabilité	Règlement (UE) 2019/817 (règlement IOP Frontières) et règlement (UE) 2019/818 (règlement IOP Police)
sBMS	Service partagé d'établissement de correspondances biométriques
SEM	Secrétariat d'État aux migrations
SG-EJPD	Secrétariat général du Département fédéral de justice et police
SIS	Système d'information Schengen
SLTD	Base de données d'Interpol sur les documents de voyage volés ou perdus (*Stolen and Lost Travel Documents Database*)
SRC	Service de renseignement de la Confédération
TDAWN	Base de données d'Interpol sur les documents de voyage associés aux notices (*Travel Documents Associated with Notices Database*)
USS	Union syndicale suisse
VIS	Système d'information sur les visas