19.xxx

Rapport explicatif

concernant la reprise et la mise en œuvre des 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 (règlements [UE] 2019/817 et [UE] 2019/818)

"Développement de l'acquis de Schengen"

du …

Aperçu

L'interopérabilité rendra possible l'échange d'informations entre les différents systèmes d'information de l'UE. Les autorités de contrôle aux frontières, de migration et de poursuite pénale pourront désormais obtenir en une seule requête des informations détaillées concernant la personne contrôlée. L'interopérabilité doit améliorer la sécurité dans l'espace Schengen, permettre des contrôles plus efficaces aux frontières extérieures et contribuer à la gestion de la migration. Ce rapport présente les mesures juridiques nécessaires en vue de la reprise et de la mise en œuvre des règlements de l'UE sur l'interopérabilité et donne un aperçu des répercussions 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 consulter séparément chaque système d'information afin d'obtenir des informations sur une personne. Ainsi les synergies ne sont pas exploitées et il existe un risque que des informations importantes ne soient pas découvertes. 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 figurent. À l'avenir, il sera possible de mener une recherche parallèlement dans plusieurs systèmes d'information à la fois. L'interopérabilité permet de reconnaître et de relier entre elles les données existantes. Les droits d'accès des autorités concernées aux différents systèmes d'information restent inchangés.

Les deux règlements de l'UE sur l'interopérabilité ont été notifiés à la Suisse en tant que développements de l'acquis de Schengen le 21 mai 2019. En signant l'accord d'association à Schengen, la Suisse s'est engagée à reprendre tous les développements de l'acquis de Schengen. La Suisse dispose de deux ans pour créer les bases légales nécessaires à la mise en œuvre de ces règlements.

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. L'interopérabilité permet également la comparaison automatisée de données biométriques ainsi que la collecte de données biographiques et biométriques de ressortissants d'États tiers dans un répertoire commun et crée de nouvelles possibilités pour découvrir la véritable identité de personnes figurant dans plusieurs systèmes d'information sous de fausses identités ou des identités multiples.

En Suisse, la mise en œuvre des deux règlements de l'UE implique de modifier des lois fédérales ainsi que le droit d'exécution y afférent. La transposition des règlements de l'UE sur l'interopérabilité implique une charge supplémentaire en termes de finances et de personnel pour l'administration fédérale et pour les cantons. Les systèmes et les processus existants en Suisse doivent être adaptés afin de pouvoir profiter des possibilités qu'offre l'interopérabilité. Parallèlement, il est prévu de mettre à disposition un instrument d'interrogation qui permettrait d'améliorer l'interopérabilité des systèmes de police nationaux et cantonaux en Suisse et de les relier au portail de recherche européen.

Table des matières

Rapport explicatif

1 Contexte

1.1 Nécessité d'agir et objectifs

En signant l'accord d'association à Schengen (AAS)[1], la Suisse s'est engagée à reprendre tous les développements de l'acquis de Schengen (art. 2, al. 3, et art. 7, AAS). La reprise d'un nouvel acte juridique a lieu dans le cadre d'une procédure spéciale qui englobe 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.

Le 20 mai 2019, le Parlement européen et le Conseil de l'Union européenne ont adopté deux règlements visant l'établissement de l'interopérabilité entre les systèmes d'information de l'UE.

- Le règlement (UE) 2019/817[2] concerne le domaine des frontières et des visas (ci-après "règlement IOP Frontières").

- Le règlement (UE) 2019/818[3] concerne le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration (ci-après "règlement IOP Police").

Aujourd'hui déjà, les autorités de contrôle aux frontières, de migration et de poursuite pénale ont accès à différents systèmes d'information de l'UE. Or ces systèmes ne sont pas reliés entre eux du point de vue technique. Les données sont enregistrées séparément dans les différents systèmes d'information. Il existe donc un risque que des synergies ne puissent pas être exploitées et que des informations et des concordances importantes ne soient pas découvertes lorsque le système dans lequel elles 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 et démontre comment l'interopérabilité permettra de combler cette faille.

Un criminel 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 renvoyée dans son pays

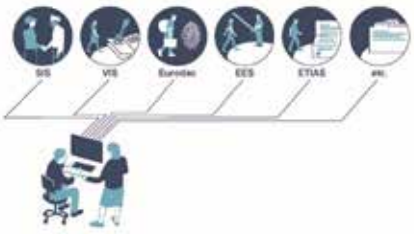
1 RS **0.362.31**

2 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

3 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

d'origine. La même personne demande par la suite un visa auprès de l'ambassade d'un autre État Schengen sous une fausse identité. Ses empreintes digitales ont certes été enregistrées dans le système central d'information sur les visas (VIS), mais elles n'ont pas été comparées avec les empreintes enregistrées dans le SIS. La personne concernée obtient un visa et réussit ainsi à retourner dans l'espace Schengen.

Grâce à l'interopérabilité entre les systèmes d'information de l'UE, les données d'identité, les données issues de documents de voyage et les données biométriques (empreintes digitales et images du visage) seront désormais automatiquement comparées. Ainsi les criminels qui opèrent sous couvert d'une fausse identité pourront être identifiés. Tous les systèmes d'information (dans ce cas le SIS et le VIS) pourront être consultés en même temps et en une seule requête via le portail de recherche européen (ESP).



Sans l'interopérabilité, chaque système devrait être consulté séparément.[4]

Grâce à l'interopérabilité, les autorités pourront consulter tous les systèmes d'information en une seule requête.

Assurer l'interopérabilité signifie donc relier les systèmes d'information de l'UE entre eux de façon à pouvoir utiliser de manière plus efficace et plus ciblée les informations qui y figurent. À l'avenir, les autorités pourront ainsi obtenir en une requête les informations pertinentes pour leurs tâches concernant une personne et se faire rapidement une idée complète de la personne en question. 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. L'UE a adopté deux règlements à cette fin. Outre la création de l'ESP, l'interopérabilité permettra également de comparer automatiquement les données biométriques d'une personne (empreintes digitales et images du visage) avec les données d'autres banques de données. Il est par ailleurs

[4] Dans les illustrations, le terme "etc." désigne les systèmes d'information et les banques de données auxquels la Suisse n'a pas directement accès actuellement mais auxquelles elle envisage de participer (ECRIS-TCN) ou auxquelles elle se prépare déjà à participer (données d'Europol, banques de données d'Interpol).

prévu de stocker dans une banque de données commune les données d'identité et les données issues de documents de voyage de ressortissants d'États tiers. Enfin, les deux règlements de l'UE offrent la possibilité de mieux détecter les identités multiples dans les systèmes d'information de l'UE et de lutter contre la fraude à l'identité. Assurer l'interopérabilité revient non pas à collecter de nouvelles données, mais plutôt à créer de nouvelles fonctions pour les systèmes d'information actuels et futurs. Rien ne change donc pour les autorités en termes de droits d'accès existants aux systèmes sous-jacents.

Les deux règlements de l'UE sur l'interopérabilité ont été élaborés suite aux attentats terroristes commis en 2015 dans l'espace Schengen et au regard des défis croissants dans le domaine migratoire. Le développement et l'élargissement des structures informatiques de l'UE sont vus comme 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 existantes en matière de sécurité. L'échange facilité des données doit cependant aussi permettre des contrôles plus efficaces aux frontières extérieures et à soutenir la prévention et 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 contrôle aux frontières, douanières, migratoires et de poursuite pénale.

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 l'acquis de Schengen dans les délais impartis et à créer les bases légales nécessaires à sa mise en œuvre.

1.2 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 juin 2018. Les sujets suivants ont donné lieu à des discussions particulièrement intenses:

- Mise en œuvre: outre les conséquences financières pour les États Schengen, il a été question des effets de l'implémentation sur les contrôles des personnes aux frontières extérieures de Schengen. Des doutes ont été exprimés en particulier quant à la faisabilité technique d'une consultation simultanée de tous les systèmes interopérables lors de contrôles aux frontières extérieures.
- Besoins accrus en termes de personnel: la question des coûts supplémentaires en termes de personnel pour les États Schengen a de nouveau été abordée, de

même que la charge supplémentaire pour les services existants tels que les bureaux SIRENE[5].

- "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 conduisent à des résultats de recherches variables dans les systèmes centraux interopérables. Cela concerne surtout le Royaume-Uni et l'Irlande, qui n'ont pas accès au SIS et qui ne peuvent donc pas profiter des fonctionnalités du détecteur d'identités multiples, mais aussi la Suisse et d'autres États associés en raison de l'accès limité aux données d'Europol ou de l'absence d'accès au système européen d'information sur les casiers judiciaires (ECRIS-TCN) pour les ressortissants d'États tiers.

Le 14 juin 2018, le COREPER[6] a défini les directives de négociation en vue du trilogue avec le Parlement européen. Sur la base des améliorations apportées au texte de compromis original, le COREPER a approuvé une nouvelle fois les textes modifiés le 12 septembre 2018 et a attribué le mandat de négociation en vue du trilogue. La Commission LIBE[7] du Parlement européen a adopté son rapport le 15 octobre 2018. Le trilogue a eu lieu d'octobre 2018 à février 2019 et s'est accompagné de réunions techniques et de rencontres des conseillers JAI. Lors des négociations en trilogue, d'autres thèmes se sont retrouvés au premier plan qu'auparavant au niveau experts, par exemple l'accès au répertoire commun de données d'identité à des fins d'identification ou de poursuite pénale, ou encore l'obligation d'information de la part des États via le portail en ligne. 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. Les experts suisses 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.

Lors du dernier trilogue, le 5 février 2019, la présidence roumaine et les représentants du Parlement européen sont parvenus à un compromis concernant les textes des règlements. Les deux règlements ont été approuvés le 13 février 2019 par le COREPER et le 19 février 2019 par la Commission LIBE du Parlement européen. 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 y 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.

5 SIRENE est l'acronyme de *Supplementary Information Request at the National Entries*. Chaque État participant au système Schengen dispose d'un bureau national opérationnel 24h sur 24 qui se charge de l'échange d'informations et de la coordination des mesures en cas de réponse positive dans le SIS.

6 Comité des représentants permanents des États membres, chargé de la préparation des travaux du Conseil de l'UE.

7 Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.

1.3 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 contraignant sur le plan légal, la notification par l'UE ainsi que 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 ont un caractère obligatoire. Aussi les présents règlements doivent-ils également 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. 7.1). 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 deux ans à compter de la notification des actes en question par le Conseil de l'UE, période dans laquelle devrait également s'inscrire un éventuel 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 aucun référendum n'est lancé 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 de mettre fin à la coopération Schengen dans son ensemble et met ainsi également en danger 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 pour la reprise et la mise en œuvre des règlements de l'UE arrive à échéance le 21 mai 2021. À

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).

noter cependant que le délai ordinaire de deux ans est prolongé pragmatiquement lorsque l'application de l'acte à l'intérieur de l'espace Schengen est prévue pour une date ultérieure. C'est le cas pour certains éléments centraux des règlements de l'UE sur l'interopérabilité, étant donné que ces derniers seront mis en service à un autre moment et que la mise en œuvre complète n'est pas prévue avant 2023.

1.4 Rapport avec le programme de la législature et la planification financière, ainsi qu'avec les stratégies du Conseil fédéral

Le projet n'a été annoncé explicitement ni dans le message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[9], ni dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[10].

La présente reprise des développements de l'acquis de Schengen contribue néanmoins à la mise en œuvre de la ligne directrice 1, objectif 4 et de la ligne directrice 3, objectifs 13 à 15 pour la législature 2015 à 2019. En utilisant de manière correcte et interopérable les différents systèmes d'information de l'UE, la Suisse développe ses relations politiques et économiques avec l'UE. Le fait de mettre rapidement et complètement les informations pertinentes à la disposition des autorités compétentes va dans le sens 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 intérieures et extérieures et posséder les instruments nécessaires pour y faire face efficacement. L'interopérabilité soutient ce travail en comblant les lacunes existantes en matière de sécurité et en rendant possibles des contrôles plus efficaces aux frontières extérieures.

Concernant la réalisation de l'interopérabilité des systèmes d'information de l'UE, une première tranche comprenant un plan intégré des tâches et des finances 2021-2023 figure au budget 2020. Une fois que les plans de gestion de projet mis à jour ainsi qu'un rapport sur la qualité des projets concernés et sur les risques qui s'y rapportent seront disponibles, le Conseil fédéral donnera le feu vert pour la deuxième tranche du crédit d'engagement "Développements Schengen/Dublin".

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

2 Principes généraux des règlements de l'UE

2.1 Vue d'ensemble

L'interopérabilité n'a pas pour but de créer des banques de données supplémentaires, mais plutôt 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 éléments centraux pour les systèmes d'information de l'UE:

9 FF **2016 1113**
10 FF **2016 981**

- le portail de recherche européen (*European Search Portal*, ci-après "ESP") permet aux autorités compétentes de consulter simultanément, en une seule requête, plusieurs systèmes d'information de l'UE;
- le service partagé d'établissement de correspondances biométriques (*Shared Biometric Matching Service*, ci-après "sBMS") permet de consulter simultanément plusieurs systèmes d'information de l'UE à l'aide de données biométriques;
- le répertoire commun de données d'identité (*Common Identity Repository*, ci-après "CIR") contient les données d'identité (par ex. nom et date de naissance), les données issues de documents de voyage et les données biométriques de ressortissants d'États tiers et facilite leur identification;
- le détecteur d'identités multiples (*Multiple Identity Detector*, ci-après "MID") détecte des liens entre des données existantes et nouvelles dans différents systèmes d'information de l'UE et contribue 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 des interdictions d'entrée et désormais aussi des décisions de renvoi;
- le système d'information sur les visas (C-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 illégale dans l'espace Schengen;
- le système européen d'information sur les casiers judiciaires de ressortissants d'États tiers (ECRIS-TCN), un système électronique permettant la transmission 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 à l'avenir passer pour demander une autorisation de voyage avant d'entrer dans l'espace Schengen;
- les données d'Europol;
- la base de données d'Interpol sur les documents de voyage volés ou perdus (*Stolen and Lost Travel Documents*, ci-après "SLTD") et celle sur les documents de voyage associés aux notices (*Travel Documents Associated with Notices*, ci-après "TDAWN").

La Suisse participe aux systèmes d'information SIS, VIS, Eurodac, EES et ETIAS, qui font tous partie de l'acquis de Schengen. Le système ECRIS-TCN ne constitue par contre pas un développement de l'acquis de Schengen et la Suisse n'y a donc pour l'heure pas accès[11]. 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 utilisée dans le présent rapport aux chapitres 1 à 3 et 6 à 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 transcrits dans le droit suisse.

Actuellement, la Suisse ne dispose pas non plus d'accès direct aux données d'Europol[12]. 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 éléments 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 d'inscrire déjà la possibilité de l'ESP aux données d'Europol dans la LEI et la LSIP. En tant qu'État membre, la Suisse possède un droit d'accès aux bases de données d'Interpol mentionnées ci-dessus.

L'interopérabilité est réglée dans deux règlements au niveau de l'UE. Le premier concerne le domaine des frontières et des visas (règlement IOP Frontières) et le second le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration (règlement IOP Police). La raison de cette répartition en deux règlements est que les dispositions s'adressent à des États dont le degré de participation à Schengen varie. Ainsi les systèmes VIS, EES et ETIAS concernent des parties de l'acquis de Schengen à laquelle l'Irlande et le Royaume-Uni ne participent pas. La Suisse est quant à elle tenue, conformément à sa participation à l'acquis de Schengen, de reprendre les deux règlements. Les deux règlements de l'UE se recouvrent à quelques exceptions près.

2.2 Entrée en vigueur des règlements sur l'interopérabilité

Les deux règlements sur l'interopérabilité sont entrés en vigueur dans l'UE le 11 juin 2019. La grande majorité des dispositions matérielles ne deviendra cependant applicable que plus tard, étant donné que la Commission européenne décide de la mise en service par étapes des différents éléments centraux et que les dispositions ad hoc ne deviennent applicables qu'à dater de cette décision (cf. art. 79 du règlement IOP Frontières et art. 75 du règlement IOP Police). Les conditions pour la mise en service des différents éléments centraux incluent par exemple le fait d'achever avec succès un test complet en collaboration avec les États Schengen et les agences européennes du composant central concerné. En outre, les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données doivent être en

[11] La Suisse examine actuellement la possibilité de participer à l'ECRIS-TCN.

[12] En vertu des art. 8 et 9 de l'accord de 2004 entre la Suisse et Europol (RS 0.362.2), la Suisse peut adresser une demande à Europol afin d'obtenir des informations du système d'information d'Europol (EIS). La Suisse s'engage pour obtenir un accès direct aux données d'Europol.

place (art. 72 du règlement IOP Frontières, art. 68 du règlement IOP Police). Les différents éléments centraux seront donc opérationnels à des moments différents. Selon le calendrier actuel de la Commission européenne, le sBMS sera mis en service d'ici 2021, le CIR d'ici 2022 et l'ESP et le MID d'ici 2023. Différentes phases de transition sont par ailleurs prévues avant que chaque composant central puisse être mis en service.

Indépendamment de cela, certaines dispositions des deux règlements de l'UE sur l'interopérabilité sont déjà valables à partir du 11 juin 2019. Il s'agit des dispositions qui sont pertinentes pour la phase de développement. Elles portent en premier lieu sur l'agence européenne eu-LISA, qui est chargée du développement des différents éléments centraux. Les bases légales déterminantes pour édicter différents actes d'exécution à l'aide desquels la Commission européenne fixera des dispositions destinées à clarifier différents aspects de réglementation sont elles aussi déjà entrées en vigueur en juin 2019. Dans ce contexte, la Suisse ne considère pas qu'il s'agit d'une "urgence particulière" justifiant l'application provisoire des deux échanges de notes au sens de l'art. 7*b* de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[13].

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. 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.

3 Contenu des règlements de l'UE

Le présent chapitre donne une vue d'ensemble du contenu des deux règlements européens, en mettant l'accent sur les quatre éléments centraux. D'autres nouveautés qui ont également des effets sur la Suisse sont exposées au ch. 3.2. Il s'agit par exemple de dispositions concernant l'obligation d'information, les exigences en matière de qualité des données et les modifications entreprises sur d'autres actes juridiques.

Étant donné que les deux règlements se recouvrent à quelques exceptions près, on a renoncé au ch. 3 à une représentation séparée et le contenu apparaît donc comme un ensemble. Les numéros de chapitres et d'articles sont pour la plupart les mêmes. Ce n'est que vers la fin du chapitre 8 des règlements de l'UE que les numéros d'articles commencent à diverger: les références sont donc indiquées séparément.

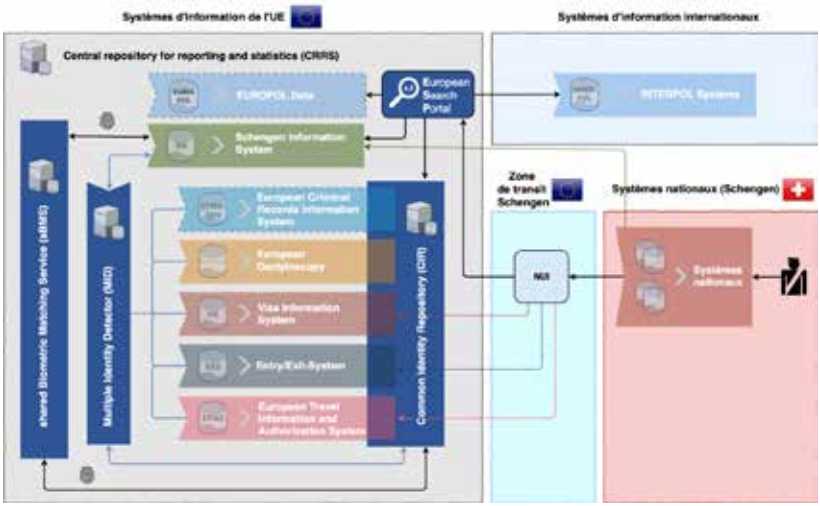
13 RS **172.010**

3.1 Les quatre nouveaux éléments centraux

Les quatre nouveaux éléments centraux forment le noyau de l'interopérabilité. Grâce à eux, les différents systèmes d'information de l'UE pourront mieux communiquer entre eux. L'échange d'informations deviendra plus efficace et les lacunes en matière de sécurité seront comblées. Les différents éléments centraux se soutiennent mutuellement. Ce n'est qu'en les combinant qu'il est 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 est possible aussi bien de consulter directement les données dans les différents systèmes que d'accéder aux données dans le CIR, où sont collectées et enregistrées les données d'identité, les données issues de documents de voyage et les données biométriques de tous les ressortissants d'États tiers qui sont enregistrées dans un des systèmes d'information non policiers de l'UE. Étant donné que les données du SIS ne sont pas intégrées dans le CIR, le MID est nécessaire pour mettre au jour des cas d'identités multiples entre le CIR et le SIS. Pour ce faire, le MID compare les données du CIR avec celles du SIS. Pour la comparaison des données biométriques, le MID a recours au sBMS; la comparaison avec les données d'identité et les données issues de documents de voyage est réalisée via l'ESP. Ensemble, les quatre éléments 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 graphique ci-dessous montre comment les éléments 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 éléments centraux de l'UE. Pour ETIAS, l'EES et le VIS, une connexion est également établie via la NUI entre le composant de l'UE concerné et les composants nationaux. Les sous-chapitres suivants exposent en détail chaque composant central de l'interopérabilité.



3.1.1 Portail de recherche européen (chapitre II)

La création du portail de recherche européen (ESP) est un point central de l'interopérabilité. Il permet 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 données d'Europol et d'Interpol (art. 6). Grâce à l'ESP, les autorités compétentes pourront à l'avenir 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 européennes autorisées à accéder au moins à l'un des systèmes d'information de l'UE (EES, ETIAS, VIS, SIS, Eurodac ou ECRIS-TCN), au CIR, au MID ou aux données d'Europol ou d'Interpol, sont habilitées à consulter l'ESP si le droit de l'UE ou le droit national prévoient des droits d'accès aux systèmes concernés et/ou aux éléments centraux. À l'avenir, 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, 21 et 22 (pour des informations détaillées sur les recherches dans le CIR, cf. ch. 3.1.3). Elles peuvent également utiliser l'ESP pour mener des recherches dans le SIS central (C-SIS)[14] ainsi que dans les données d'Europol et les banques de données d'Interpol. Pour les autori-

14 Les requêtes via l'ESP concernent toujours le SIS central, qui se trouve à Strasbourg. Aucune requête ne peut être menée dans les copies nationales.

tés des États Schengen, ceci ne constitue pas une obligation. Les services de l'UE sont en revanche tenus de mener à l'avenir leurs recherches dans le C-SIS via l'ESP.

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

En collaboration avec les États Schengen, l'agence eu-LISA crée un profil basé sur chaque catégorie d'utilisateurs de l'ESP. Chaque profil contient notamment des informations indiquant quels systèmes d'information de l'UE, données d'Europol et bases de données d'Interpol peuvent être interrogés par l'utilisateur en question. Les profils des utilisateurs sont 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 peut être menée via l'ESP sur la base de données d'identité, de données relatives à des documents de voyage ou de données biométriques. L'ESP interroge l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN et le CIR ainsi que les données d'Europol et les bases de données d'Interpol, simultanément, conformément au profil d'utilisateur. Dès que des données sont disponibles dans l'un de ces systèmes, elles sont rendues visibles à l'utilisateur via l'ESP dans la limite de ses droits d'accès. L'utilisateur voit également de quel système d'information de l'UE ou de quelle base de données proviennent les données, sauf s'il s'agit d'une requête du CIR pour identification en vertu de l'art. 20. Dans ce cas d'espèce, il s'agit simplement d'identifier une personne, mais sans que les autorités de police compétentes n'apprennent dans quel système elle est enregistrée (cf. ch. 3.1.3 relatif à l'art. 20). Lors de consultations du CIR conformément à l'art. 22, les autorités de poursuite pénale peuvent uniquement voir si des données concernant une personne figurent dans un système d'information. L'accès doit être demandé séparément (cf. ch. 3.1.3 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 doivent tenir des registres de toutes les requêtes menées via l'ESP. Les registres ne peuvent être utilisés que pour contrôler la protection des données. Ils doivent être protégés des accès non autorisés et être 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 notifie de manière automatisée aux utilisateurs de l'ESP. En cas de défaillance de l'infrastructure nationale d'un État Schengen, ce dernier le notifie de manière automatisée à l'eu-LISA et à la Commission européenne. Jusqu'à ce que qu'il soit remédié à la défaillance technique, les

États membres peuvent 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 une période de deux ans à compter de la mise en service du composant central. Ce délai peut être prolongé une seule fois et d'une année au maximum.

3.1.2 Service partagé d'établissement de correspondances biométriques (chapitre III)

Le Service partagé d'établissement de correspondances biométriques (sBMS[15]) permettra d'effectuer des recherches simultanées dans plusieurs systèmes d'information de l'UE à l'aide de données biométriques (art. 12).

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

Le sBMS stocke les modèles biométriques[16] qu'il génère à partir des données biométriques de l'EES, du VIS, du SIS de l'ECRIS-TCN et, à une date ultérieure, d'Eurodac. ETIAS n'est pas concerné, puisqu'il ne contient pas de données biométriques. Chaque modèle contient une référence aux systèmes d'information de l'UE dans lesquels les données biométriques correspondantes sont stockées et une référence aux enregistrements concrets qui y figurent. Seuls les modèles biométriques respectant une norme minimale de qualité peuvent 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 fait par le biais des modèles biométriques dans le sBMS et n'est autorisée que conformément aux finalités prévues dans les règlements sur l'interopérabilité ainsi que dans les règlements de l'UE relatifs aux différents systèmes.

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 elles sont issues ne sont stockés dans le sBMS qu'aussi longtemps que les données

[15] Les deux règlements de l'UE utilisent le terme "BMS", qui est déjà en usage dans un autre contexte dans la législation suisse. Afin d'éviter les confusions, on utilisera donc ici le terme "sBMS".

[16] Il s'agit d'une représentation mathématique obtenue par l'extraction de caractéristiques des données biométriques, se limitant aux caractéristiques nécessaires pour procéder à des identifications et à des vérifications (art. 4, par. 12).

biométriques correspondantes sont stockées dans le CIR ou le SIS. Ils sont ensuite effacés de manière automatisée.

Tenue de registres (art. 16)

L'eu-LISA et les États Schengen sont tenus de tenir des registres de toutes les opérations de traitement de données. Les dispositions relatives à l'utilisation des registres et des mesures de sécurité à prendre présentées au ch. 3.1.1 concernant l'art. 10 s'appliquent par analogie.

3.1.3 Conservation des données dans le service partagé d'établissement de correspondances biométriques (chapitre IV)

Un dossier individuel est créé dans le CIR pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac ou l'ECRIS-TCN. L'objectif est de faciliter l'identification des personnes qui sont enregistrées dans l'un de ces systèmes d'information. Le CIR permet notamment de simplifier et d'améliorer l'accès des autorités de poursuite pénale aux systèmes d'information de l'UE non consacrées 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 avec renvoi à l'art. 22). Les données du SIS ne font pas partie du CIR, en raison de son architecture technique complexe.

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

Le CIR enregistre les données d'identité ainsi que, si elles sont disponibles, les données relatives aux documents de voyage et les données biométriques issues de l'EES, du VIS, d'ETIAS, de l'ECRIS-TCN et, à une date ultérieure, d'Eurodac. Le CIR stocke les données selon une séparation logique en fonction du système d'information d'où elles proviennent. Pour chaque ensemble de données enregistré, le CIR comporte une référence aux systèmes d'information de l'UE auxquels appartiennent les données. Les droits d'accès des autorités au CIR dépendent du droit national, des instruments juridiques qui régissent les systèmes d'information de l'UE et des droits d'accès prévus aux règlements sur l'interopérabilité pour les fins visées aux art. 20, 21 et 22.

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

Lorsque des données sont ajoutées, modifiées ou supprimées dans l'EES, le VIS, ETIAS, l'ECRIS-TCN et, à une date ultérieure, d'Eurodac, les données enregistrées dans le CIR sont adaptées automatiquement. Lorsqu'un lien blanc ou rouge est créé dans le MID concernant des données du CIR (pour plus de détails à ce sujet, cf. ch. 3.1.4), au lieu de créer un nouveau dossier individuel, le CIR ajoute 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 consulter des données d'identité dans le CIR à certaines conditions par le biais de l'ESP. Le par. 1 établit la liste des cas dans lesquels cela 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 l'identité de cette personne, 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 ou refuse de le faire. Une interrogation du CIR pour identification ne peut viser un mineur de moins de 12 ans que si cela est dans l'intérêt supérieur de l'enfant.

Normalement, l'interrogation du CIR se fait à l'aide des données biométriques de la personne relevées en direct lors d'un contrôle d'identité (par. 2). Lorsque les données biométriques de la personne ne peuvent pas être utilisées ou lorsque la requête introduite avec ces données échoue, la requête est 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 est habilitée à les consulter, mais sans que le système n'affiche de quel système d'information de l'UE elles proviennent. Le par. 4 prévoit que les données du CIR peuvent être utilisées pour l'identification de victimes d'attentats terroristes, d'accidents ou de catastrophes naturelles ou de 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 cette 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 rapport avec les liens MID (pour des informations plus détaillées, cf. ch. 3.1.4). 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, les autorités compétentes sont autorisées à accéder aux données reliées entre elles dans le CIR.

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 désignées par chaque pays en fonction des bases légales des différents systèmes n'ont pas d'accès direct aux données dans l'EES, le VIS, ETIAS ou Eurodac mais doivent le demander auprès d'un point d'accès central qui a également été désigné par le pays.

Avec l'interopérabilité, l'accès des autorités de poursuite pénale aux données figurant dans ces systèmes doit être nouvellement réglementé. 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 peuvent consulter le CIR. Cette première étape se fait selon le procédé 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 signale aux autorités compétentes dans quel système d'information de l'UE les données figurent. Les autorités désignées ou Europol doivent ensuite rédiger une demande d'accès complet à au moins un des systèmes d'information en lien avec la réponse positive. Les autorités désignées doivent déposer une demande auprès du point d'accès central. L'autorisation d'accès complet aux données concernées dans l'EES, ETIAS, le VIS ou Eurodac reste soumise aux conditions et procédures fixées dans les instruments juridiques des systèmes d'information sous-jacents. Si, à titre exceptionnel, l'accès complet n'est pas demandé, cela doit être dûment justifié et consigné.

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

Les données sont 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 n'est stocké dans le CIR qu'aussi longtemps que les données correspondantes sont stockées dans au moins un des systèmes d'information de l'UE.

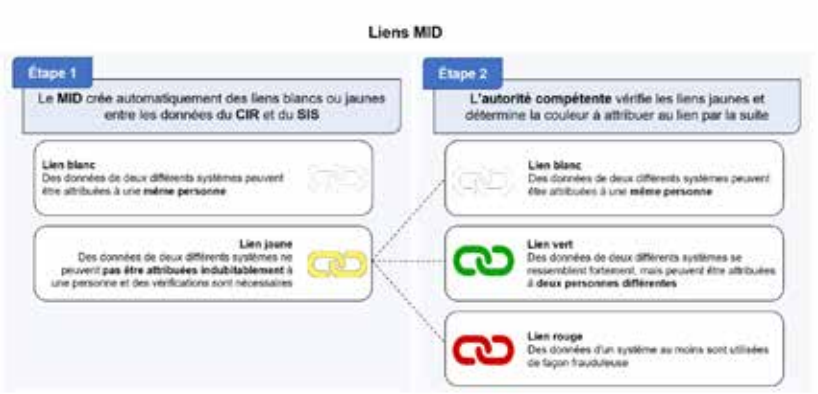
Tenue de registres (art. 24)

L'eu-LISA tient des registres de toutes les opérations de traitement de données et requêtes dans le CIR. Les États Schengen doivent tenir des registres sur les requêtes menées conformément aux art. 20, 21 et 22, et Europol sur les accès conformément aux art. 21 et 22. Les dispositions concernant l'utilisation des registres et des mesures de sécurité à prendre qui sont décrites au ch. 3.1.1 au sujet de l'art. 10 s'appliquent par analogie.

3.1.4 Détecteur d'identités multiples (chapitre V)

Le détecteur d'identités multiples (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 crée et stocke des dossiers de confirmation d'identité contenant des liens entre les données des systèmes d'information de l'UE (art. 25). Concrètement, le MID examine si les données personnelles, données relatives aux documents de voyage ou données biométriques existent déjà dans d'autres systèmes. Suivant la combinaison, le MID établit automatiquement des liens dits "blancs" ou "jaunes". Tous les liens jaunes doivent être vérifiés manuellement par les autorités compétentes: ces dernières contrôlent les différentes identités et, suivant

s'il s'agit de la même personne ou d'une autre personne déjà répertoriée dans un système d'information de l'UE, le lien est ensuite catégorisé comme rouge, vert ou blanc. Le graphique ci-dessous fournit une première vue d'ensemble de ces processus. La procédure exacte et la signification des liens seront 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 sont autorisées à y accéder aux fins de la vérification manuelle de différentes identités conformément à l'art. 29. Il s'agit des autorités qui saisissent ou mettent à jour des données dans l'EES, le VIS, ETIAS, l'ECRIS-TCN, le SIS et, à une date ultérieure, Eurodac. Ces autorités sont désignées dans les bases légales des différents systèmes d'information. D'autre part, les autorités des États Schengen et les services de l'UE ont accès aux liens rouges s'ils ont accès à au moins un système d'information de l'UE concerné, ainsi qu'aux liens blancs ou verts s'ils 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 est déclenché lors de chaque saisie ou mise à jour de données dans l'un des systèmes d'information de l'UE. Pour ce faire, les nouvelles données sont comparées avec celles figurant déjà dans le CIR et le SIS. Le sBMS se charge de la comparaison des données biométriques et l'ESP de celle des données d'identité et des données relatives aux documents de voyage. Une détection d'identités multiples n'est lancée que pour comparer des données entre les différents systèmes d'information de l'UE. Une telle recherche à l'intérieur d'un même système est exclue.

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 légales 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 ayant déclenché la correspondance. Si ces données sont déjà liées, le lien existant est étendu aux nouvelles données.

Lorsque les données d'identité dans les dossiers liés sont les mêmes 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 égales ou similaires sont définis par la Commission européenne et fixés dans un acte délégué. 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, 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 définit une exception à cette règle générale. Lorsqu'il s'agit de vérifier un lien avec un signalement du SIS conformément aux art. 26, 32, 34 ou 36[17] du règlement (UE) 2018/1862[18], le bureau SIRENE de l'État Schengen qui a créé le signalement est responsable de la vérification manuelle. 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 classifiant comme lien vert, rouge ou blanc conformément aux art. 31, 32 et 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 initiée en présence de la personne concernée et cette dernière doit avoir la possibilité de s'exprimer quant à 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 douze heures.

En cas de création de plusieurs liens, chacun d'entre eux doit être vérifié. Les autorités responsables doivent, lorsqu'elles examinent si un nouveau lien doit être créé, évaluer si les données ayant généré une correspondance sont déjà liées.

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 suite à un 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.

17 Il s'agit des catégories de signalement suivantes:
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.

18 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.

Lien vert (art. 31)

Un lien n'est classifié 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. Cela peut être le cas par exemple 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.

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 effacer 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 classifié comme rouge qu'une fois que la vérification manuelle a eu lieu. Il indique qu'il s'agit d'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: dans ce cas, les mêmes données biométriques ou les mêmes données relatives au 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: dans ce cas, les données liées comportent des données biométriques différentes, mais les données relatives au document de voyage sont les mêmes; les données liées se rapportent à deux personnes différentes.

- Une personne se fait passer pour une autre: dans ce cas, 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. D'éventuelles mesures ne peuvent être prises que dans le respect du droit de l'Union 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.

Lorsqu'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 (pour ce faire on lui fournit le numéro d'identification unique et l'adresse du portail en ligne, cf. ch. 3.2). L'autorité peut renoncer à informer la personne concernée si cela s'avère nécessaire afin d'assurer le respect 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 ayant 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.

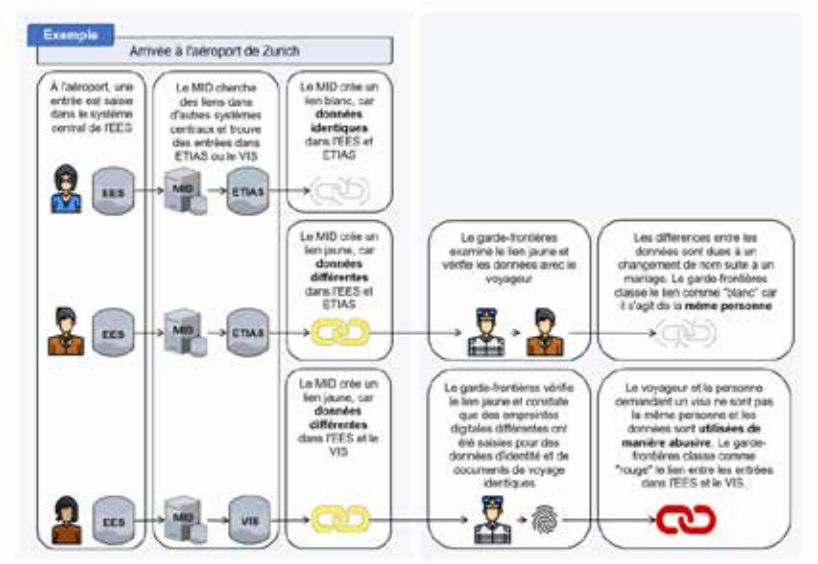
Lien blanc (art. 33)

Un lien blanc apparaît soit automatiquement lors de la détection d'identités multiples par le MID conformément à 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 conformément à 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. 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 (en lui fournissant un numéro d'identification unique et l'adresse du portail en ligne). Comme pour les liens rouges, l'autorité peut renoncer à informer la personne si cela s'avère nécessaire 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 informé 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 stockées dans au moins deux systèmes d'information de l'UE. Ils sont effacés du MID de manière automatisée.

Tenue de registres (art. 36)

L'eu-LISA et les États Schengen doivent tenir des registres de toutes les opérations de traitement de données. Les dispositions relatives à l'utilisation des registres et des mesures de sécurité présentées au ch. 3.1.1 concernant 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 déjà dans l'EES, le VIS, Eurodac et le SIS devront être vérifiées avant la mise en service pour tous pour y détecter d'éventuelles identités multiples. L'unité centrale ETIAS est chargée de cette vérification. 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 est impliqué dans la procédure de vérification. Ce n'est qu'une fois tous les liens jaunes vérifiés et leur statut mis à jour comme vert, blanc ou rouge que l'unité centrale ETIAS informe la Commission européenne. Cette dernière décide ensuite de la mise en service effective du MID. Cette vérification devrait être achevée dans un délai d'un an. Une prolongation est néanmoins possible.

3.2 Autres dispositions

Outre les dispositions relatives aux quatre éléments centraux qui constituent la majeure partie des deux règlements sur l'interopérabilité, ces règlements comprennent également de nombreuses autres dispositions, dont le contenu est résumé ci-après. À noter cependant que certaines des dispositions mentionnées ne seront mises en œuvre en Suisse qu'au niveau de l'ordonnance, voire n'ont pas besoin d'être reprises dans le droit suisse.

Mesures soutenant l'interopérabilité (chapitre VI)

Afin de rendre possible l'interopérabilité des différents systèmes d'information de l'UE, les mesures de soutien suivantes 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 éléments 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). Ce dernier sert à fournir des statistiques intersystèmes. À cette fin, les données sont rendues anonymes, si bien que l'identification d'individus n'est pas possible.

Protection des données (chapitre VII)

Le chapitre VII est entièrement consacré à la protection des données. Il établit la liste des services responsables du traitement des données d'une part (art. 40) et de la

sécurité du traitement des données d'autre part (art. 42). L'eu-LISA remplit une fonction importante dans ce domaine, puisque cette agence est responsable de la sécurité des éléments 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 éléments 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 à savoir 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 une demande de rectification ou d'effacement de données à caractère personnel est adressée à un État qui n'est pas compétent en matière de vérification manuelle de différentes identités, ce dernier prend contact avec l'État Schengen compétent ou avec l'unité centrale ETIAS, si cette dernière est chargée de la vérification. Cette vérification doit en général avoir lieu dans les 45 jours suivant la réception de la demande. Une prolongation est cependant 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. 34c permet notamment de connaître l'autorité compétente de l'État Schengen concerné. 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 dans les éléments centraux, traitées ou accessibles par ces éléments, ne peuvent en principe pas être transférées vers un pays tiers, une organisation internationale, une entité privée ou une personne phy-

sique ou être mises à leur disposition (art. 50). Conformément à l'art. 50, cela s'applique sous réserve des dispositions en matière de protection des données concernant le transfert de données dans les bases légales des systèmes de l'UE concernés par l'interopérabilité 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 contrôle ainsi que les audits par le Contrôleur européen de la protection des données. Les États Schengen doivent veiller à ce que les autorités de contrôle 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 quatre 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 éléments centraux et de l'application d'autres dispositions des règlements sur l'interopérabilité (art. 53). Tous les deux 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 (chapitre 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 chargé du développement des éléments 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. Il est garanti que l'eu-LISA n'a 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 éléments 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 (chapitre IX)

Les règlements de l'UE sur l'interopérabilité entraînent des modifications d'autres instruments. Il s'agit de règlements que la Suisse a déjà repris au moyen d'un

échange de notes, ou pour lesquelles une procédure de reprise est en cours. Il s'agit du règlement (CE) n° 767/2008 sur le VIS, du règlement (UE) 2016/399 sur le code frontières Schengen, du règlement (UE) 2017/2226 sur l'EES, du règlement (UE) 2018/1240 sur ETIAS, du règlement (UE) 2018/1726 sur l'eu-LISA, du règlement (UE) 2018/1861 sur le SIS, de la décision 2004/512 /CE sur la mise en place du VIS ainsi que de la décision 2008/633/JAI concernant l'accès des autorités de poursuite pénale au VIS. 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. La Suisse n'est cependant pas liée par ce dernier.

Les modifications sont nécessaires afin de pouvoir exploiter pleinement les nouvelles possibilités qu'offre l'interopérabilité. Il s'agit en particulier de définir les catégories de données qui seront stockées ou saisies dans les éléments centraux et de prévoir la connexion des différents systèmes aux nouveaux éléments centraux.

Dispositions finales (chapitre X)

Le dernier chapitre contient des dispositions concernant les périodes transitoires pour l'utilisation des différents éléments centraux, ainsi que les tâches des différentes autorités qui doivent être remplies pour ce faire[19] (art. 67 à 69 du règlement IOP Frontières ou art. 63 à 65 du règlement IOP Police). Sont également réglés dans ces chapitres la mise en service (art. 72 du règlement IOP Frontières ou art. 68 du règlement IOP Police), la formation des autorités compétentes (art. 76 du règlement IOP Frontières ou art. 72 du règlement IOP Police), le suivi et l'évaluation du développement et du fonctionnement des éléments centraux (art. 78 du règlement IOP Frontières ou art. 74 du règlement IOP Police) et l'entrée en vigueur (art. 79 du règlement IOP Frontières ou art. 75 du règlement IOP Police).

4 Présentation de l'acte de mise en œuvre

4.1 Réglementation proposée

Le projet porte sur la reprise d'un développement de l'acquis de Schengen. Sa transposition dans le droit suisse nécessite une modification de lois fédérales et, plus tard, d'ordonnances y afférentes (cf. ch. 4.3.1).

4.2 Adéquation des moyens requis

La mise en œuvre en Suisse des règlements de l'UE sur l'interopérabilité s'accompagne de charges financières et en personnel pour l'administration fédérale et les cantons. Ces charges, spécifiées au ch. 6, doivent toutefois être mises en regard des grands avantages que devraient apporter les nouvelles possibilités introduites par les deux textes européens. Les informations disponibles pourront être utilisées de ma-

19 Le contenu de ces dernières est cité aux chapitres dédiés aux différents éléments centraux au ch. 3.1.

nière plus efficace et ciblée, soit une importante valeur ajoutée pour le travail des autorités de contrôle aux frontières, de migration et de poursuite pénale. L'interopérabilité accroîtra la sécurité dans l'espace Schengen.

4.3 Mise en œuvre

4.3.1 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. Le présent chapitre détaille les nouveautés requérant une modification de lois fédérales. De nombreux changements en revanche n'ont 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'élargiront pas les droits d'accès actuels de chaque autorité aux systèmes sous-jacents ni ne changeront les dispositions quant à la finalité des systèmes d'information européens. Bien plus, par exemple, le portail en ligne viendra créer de nouvelles possibilités qui faciliteront la communication entre les autorités nationales compétentes sur les personnes enregistrées. L'accès à des données personnelles sensibles restera donc clairement réglementé, même après la reprise des deux règlements européens.

Les éléments centraux relient les systèmes d'information régis dans la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[20] ainsi que les banques de données de police régies dans la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[21]. Par souci de transparence, ils doivent être réglementés en conséquence dans ces deux lois s'ils concernent des systèmes d'information dont la base formelle légale est actuellement contenue dans l'une de ces deux lois. Ils sont réglementés dans l'ordre correspondant à leur mise en service prévue (le sBMS d'abord, suivi du CIR, de l'ESP et du MID).

L'introduction des éléments centraux entraîne des adaptations dans la structure de la LEI comme de la LSIP.

La nécessité concrète de modifier chacune des lois est résumée ci-après (cf. ch. 5 pour le commentaire des dispositions).

Loi sur les étrangers et l'intégration

Certaines dispositions à mettre en œuvre dans le droit suisse nécessitent des modifications de la LEI.

L’expression "systèmes d’information Schengen-Dublin" est introduite du fait que les systèmes d’information réglementés dans la LEI sont régis par l’accord d’association à Dublin, de même que pour éviter toute confusion avec le "système d’information Schengen N-SIS".

20 RS **142.20**
21 RS **361**

Les chapitres 14 à 14*c* LEI doivent être réorganisés eu égard à l'introduction d'éléments 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.

Du fait que neuf règlements de l'UE ont dû être modifiés en vue de la mise en place de l'interopérabilité des systèmes d'information (ETIAS, EES, SIS, cf. ch. 3.2), les dispositions correspondantes de la LEI qui régissent aujourd'hui ces 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, de l'ETIAS, 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, tels que VIS, Eurodac, EES et ETIAS, de telle sorte que de nouvelles données alphanumériques (données d'identité et données relatives aux documents de voyage) et biométriques des différents systèmes seront 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 le CIR.

En outre, les différents éléments de l'interopérabilité doivent être réglementés. Il s'agira en particulier d'en définir le contenu et de fixer les règles d'accès à ces éléments centraux (BMS partagé à l'art. 110 ; CIR à l'art. 110*a* ; MID à l'art. 110*f*). Cette démarche est conforme à l'art. 17, al. 1, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[22], qui prévoit que les organes fédéraux ne peuvent traiter des données personnelles que s'il existe une base légale formelle.

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* ; détection d'infractions pénales à l'art. 110*d*. Dans ce dernier cas, les autorités désignées, en particulier le 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 « hit / no hit » conformément à l'art. 22 des règlements de l'UE sur l'interopérabilité). Des autorités policières doivent être désignées pour les accès à des fins d'identification. Il convient également de 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 règlementés.

La communication de données aux entités autorisées (art. 110*h*), la responsabilité du traitement des données dans le BMS partagé, 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 C-VIS, l'EES et l'ETIAS doivent être modifiées.

22 RS **235.1**

Il faut s'attendre à d'autres détails et 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 là aussi être mis en œuvre au niveau de l'ordonnance.

Enfin, les renvois aux règlements européens dans la loi doivent être actualisés.

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

Dans la LDEA[23], certains renvois à des dispositions de la LEI touchées par la présente révision doivent être modifiées. Ces adaptations n'entraînent aucune modification matérielle de la LDEA.

Loi sur la responsabilité

Actuellement, la loi du 14 mars 1958 sur la responsabilité (LRCF)[24] réglemente le SIS aux art. 19*a* et *b*. Les bases légales 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 pas un assemblage de données au sens de l'art. 3, let. d, LPD puisqu'aucune donnée personnelle n'y figure. Le terme "composant" est donc lui aussi introduit, et il n'est plus seulement question de "système d'information".

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

Comme indiqué en introduction au présent chapitre, la LSIP, qui régit les bases légales 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 personnelles 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 doivent donc être inscrits dans cette dernière. Sont concernés les éléments centraux qui englobent le SIS.

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

Étant donné que plusieurs articles concernant le traitement des données dans les systèmes d'information Schengen-Dublin doivent être introduits, la systématique de la LSIP est modifiée. Lesdits systèmes ou leurs composants figurent désormais dans une section distincte (nouvelle section 4). Ils sont réglementés dans l'ordre correspondant à leur mise en service prévue (le sBMS à l'art. 18*a*, l'ESP à l'art. 18*b* et le MID à l'art. 18*c*).

23 SR **142.51**
24 RS **170.32**

Depuis l'entrée en vigueur le 1er mars 2019 de la loi fédérale mettant en œuvre la directive (UE) 2016/680[25], l'art. 349*c* CP réglemente la communication de données personnelles à un État tiers ou à un organisme international[26]. 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)[27], 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[28]. 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 transposition des règlements européens. 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. 18*e*). La responsabilité du traitement des données dans les systèmes d'information Schengen-Dublin ou leurs composants doit elle aussi être réglementée (art. 18*f*).

4.3.2 Évaluation prévue de l'exécution

Chaque État Schengen est évalué tous les cinq ans au moins quant à la mise en œuvre et à l'application du droit Schengen. La Suisse a été évaluée à trois reprises à ce jour: en 2008 en vue de la participation à la coopération opérationnelle, en 2014 et en 2018. L'évaluation porte sur la coopération policière, SIS/SIRENE, les frontières extérieures, le retour, la protection des données et les visas. Elle concerne tant la Confédération que les cantons. Après des inspections sur place, les experts rédigent un rapport où figurent les éventuelles insuffisances. Afin de remédier à ces dernières, le Conseil de l'UE peut adresser des recommandations concrètes à la Suisse, qui, à son tour, rend compte à l'UE des mesures qu'elle a prises par suite de ces recommandations. Les futures évaluations porteront également sur la mise en œuvre des règlements de l'UE sur l'interopérabilité.

25 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, version du JO L 119 du 4.5.2016, p. 89

26 RO **2019** 625

27 RS **360**

28 RO **2019** 625

5 Commentaire des dispositions de l'acte de mise en oeuvre

5.1 Loi fédérale sur les étrangers et l'intégration

Art. 5 Abs. 1 Bst. a^{bis}, note de bas de page

Vu que le règlement (UE) 2018/1240[29] portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) est modifié par le règlement (UE) 2019/817 (« Interopérabilité frontières et visas »), la note de bas de page de l'art. 5, al. 1, let. a^{bis}, doit être modifiée en conséquence.

Cette disposition doit, par ailleurs, être coordonnée avec l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'autorisation et d'information concernant les voyages (ETIAS) (développement de l'acquis Schengen)[30].

Art. 7, al. 3, note de bas de page

Vu que le code frontières Schengen (CFS)[31] est modifié par le règlement (UE) 2019/817 (« Interopérabilité frontières et visas »), la note de bas de page figurant à l'art. 7, al. 3, doit être modifiée en conséquence.

Cette disposition doit, par ailleurs, être coordonnée avec l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'autorisation et d'information concernant les voyages (ETIAS) (développement de l'acquis Schengen).

Art. 9a

L'art. 9*a* reprend sans modification matérielle le contenu de l'actuel art. 103 LEI. Il traite de la surveillance de l'arrivée à l'aéroport. Ce changement impose de modifier les références à l'art. 1, al. 2, LDEA.

Art. 68a, al. 2, note de bas de page

Le règlement (UE) 2018/1861[32] étant modifié par le règlement (UE) 2019/818 (« Interopérabilité policière et judiciaire »), la note de bas de page de l'art. 68*a*, al. 2, doit être modifiée en conséquence.

29 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) n° 1077/2011, (UE) n° 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 (UE) 2019/817, JO L 135 du 22.5.2019, p. 27

30 Ce projet a été en consultation du 13 février 2019 au 20 mai 2019.

31 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, modifié en dernier lieu par le règlement (UE) 2019/817, JO L 135 du 22.5.2019, p. 27

Cette disposition doit par ailleurs être coordonnée avec l'arrêté fédéral portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases juridiques sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) (règlements [UE] 2018/1862, 2018/1861 et 2018/1860 (développements de l'acquis de Schengen)[33].

Art. 92a

L'art. 92*a* reprend sans modification matérielle le contenu de l'actuel art. 104 LEI. Il traite de l'obligation des entreprises de transport aérien de communiquer des données personnelles. Ce changement impose de modifier les références qui figurent aux art. 104*a*, al. 1bis, 2, 3, 3bis, 4 et 5, 104*b*, al. 1, 122*b*, al. 2 et 122*c*, al. 3, let. b.

Protection et traitement des données

Au vu de la mise en place de nouveaux éléments centraux ayant une incidence sur l'ensemble des systèmes d'information Schengen-Dublin, il convient de réorganiser les chap. 14 à 14*c*:

- Le chap. 14 devra désormais contenir toutes les dispositions relatives à la protection et au traitement des données en général.
- Le chap. 14*a* devra désormais réglementer tous les systèmes d'information (ceux du SEM et ceux liés à Schengen).
- Le chap. 14*b*, qui portait jusqu'à présent sur les dispositions relatives à 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.
- Le chap. 14*c*, qui portait jusqu'à présent sur les dispositions relatives à 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 au chap. 14*a* (section à part consacrée à Eurodac).

Chapitre 14 Traitement et protection des données

Le chap. 14 voit son titre modifié. Il ne réglemente plus que la protection et le traitement 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

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) n° 1987/2006, JO L 312 du 7.12.2018, p. 14, modifié en dernier lieu par le règlement (UE) 2019/818, JO L 135 du 22.5.2019, p. 85.

33 Ce projet a été en consultation du 13 février 2019 au 20 mai 2019.

titres de séjour) et 102*b* (Contrôle de l'identité du détenteur d'un titre de séjour biométrique) LEI, le chap. 14 comprend désormais également:

- l'art. 102*c* (Communication de données personnelles à l'étranger);
- l'art. 102*d* (Communication de données personnelles à l'État d'origine ou de provenance);
- l'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'actuel art. 105 LEI. 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'actuel art. 106 LEI. 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'actuel art. 107 LEI. Il traite de la communication de données personnelles dans le cadre des accords de réadmission et de transit.

Art. 103

Il est ici fait renvoi au commentaire de l'art. 9a.

Chapitre 14a Systèmes d'information

Le chap. 14*a* figure désormais avant l'art. 103*a* LEI (INAD). Il traite des systèmes d'information suivants:

- Section 1 (Système d'information sur les refus d'entrée [système INAD]): art. 103*a* LEI;
- Section 2 (Système d'entrée et de sortie [EES] et contrôle automatisé à la frontière): art. 103*b* à 103*g* LEI;
- Section 3 (Système d'information des passagers [système API]): art. 104*a* à 104*c* et 108 LEI (l'art. 108 LEI étant déjà abrogé);
- Section 4 (Système européen d'information et d'autorisation concernant les voyages [ETIAS]): art. 108*a* à 108*g* et 109 LEI (l'art. 109 LEI étant déjà abrogé);

- Section 5 (Système central d'information sur les visas [C-VIS] et système national d'information sur les visas [ORBIS]): art. 109*a* à 109*e* LEI;
- Section 6 (Système d'information destiné à la mise en œuvre des retours[34]): art. 109*f* à 109*j* LEI;
- Section 7 (Eurodac): art. 109*k* LEI;
- Section 8 (Système de gestion des dossiers personnels et de la documentation): art. 109*m* LEI.

Section 1 Système d'information sur les refus d'entrée

Une section intitulée *Système d'information sur les refus d'entrée* a été ajoutée avant l'art. 103*a*.

Art. 103a

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

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

Une section a été ajoutée avant l'art. 103*b*. Elle comporte des dispositions relatives au système d'entrée et de sortie (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

Al. 1, note de bas de page

Le règlement (UE) 2017/2226[35] portant création d'un système d'entrée/de sortie (EES) étant modifié par le règlement (UE) 2019/817 (« Interopérabilité frontières et visas »), la note de bas de page de l'art. 103*b*, al. 1, doit être modifiée en conséquence.

Cette disposition doit par ailleurs être coordonnée avec l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'autorisation et d'information concernant les voyages (ETIAS) (développement de l'acquis de Schengen).

34 RO **2019** 1413

35 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

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}. Une référence précise, à l'al. 4, aux données désormais stockées dans le CIR devient ainsi possible. L'expression *données alphanumériques* est remplacée par *données d'identité et données relatives aux documents de voyage*.

Al. 4

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

Art. 103d, titre et al. 3

Comme le CIR devient un élément de l'ETIAS, les dispositions relatives à la communication des données issues de l'EES s'appliquent aussi aux données de l'EES stockées dans le CIR (données d'identité, données relatives aux documents de voyage et données biométriques). Pour cette raison, il convient d'ajouter *CIR* dans le titre. En ce qui concerne la communication de données de l'EES qui sont stockées dans le CIR, l'al. 3 fait référence à l'art. 110*h*, lequel renvoie à son tour à l'art. 40 des deux règlements (UE) 2019/817 et (UE) 2019/818 (cf. commentaire relatif à l'art. 110*h* et ch. 3.2 Protection des données).

Art. 104

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

Section 3: Système d'information sur les passagers (système API)

Une nouvelle section est ajoutée avant l'art. 104*a*. Elle porte sur les dispositions relatives au système d'information sur les passagers API (art. 104*a* à 104*c*). Certaines dispositions de cette section doivent subir des modifications d'ordre formel. Elles ne subissent pas de modification matérielle.

Art. 104a, titre et al. 1bis, 2, 3, 3bis, 4 et 5

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 à 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*.

Chap. 14, section 3 (art. 105 à 107)

Abrogée

La section 3 du chap. 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 européen d'information et d'autorisation concernant les voyages (ETIAS)

Une nouvelle section est ajoutée avant l'art. 108*a*. Elle porte sur les dispositions relatives au système européen d'information et d'autorisation concernant les voyages, l'ETIAS (art. 108*a* à 108*g*, l'art. 109 étant déjà abrogé).

Art. 108a, al. 1, let. a, et al. 3

Al. 1, let. a

La let. a de l'al. 1 précise que les données personnelles sont les données d'identité et les données relatives aux documents de voyage. Elles sont désormais stockées dans le CIR.

Al. 3

L'al. 3 précise quelles données sont transmises et stockées dans le CIR (cf. commentaire relatif à l'art. 110*a*). Les données d'identité et les données relatives aux documents de voyage (art. 108*a*, al. 1, let. a) sont conservées dans le CIR. Les informations relatives aux demandes d'autorisation de voyage ETIAS approuvées ou rejetées et les données figurant sur la liste de surveillance ne sont pas transmises au CIR ; elles continuent de n'être stockées que dans l'ETIAS.

Art. 108f, titre et al. 3

Vu que le CIR devient un élément de l'ETIAS, les dispositions relatives à la communication de données issues de l'ETIAS s'appliquent également aux données de l'ETIAS stockées dans le CIR (données d'identité, données relatives aux documents de voyage et données biométriques). Pour cette raison, il convient d'ajouter *CIR* dans le titre. En ce qui concerne la communication de données de l'ETIAS qui sont stockées dans le CIR, l'al. 3 fait référence à l'art. 110*h*, lequel renvoie à son tour à l'art. 40 des deux règlements (UE) 2019/817 et (UE) 2019/818 (cf. commentaire relatif à l'art. 110*h* et ch. 3.2 Protection des données).

Section 5 *Système central d'information sur les visas (C-VIS) et système national d'information sur les visas (ORBIS)*

Une nouvelle section est ajoutée avant l'article 109*a*. Elle porte sur les règles applicables au système central d'information sur les visas et au système national d'information sur les visas ORBIS (art. 109*a* à 109*e* et 109*f* à 109*j*, les art. 109*f* à 109*j* étant déjà abrogés).

Art. 109a, titre et al. 1, note de bas de page, et 1bis

Al. 1, note de bas de page

Étant donné que le règlement (CE) n° 767/2008 concernant le système d'information sur les visas (VIS)[36] a été modifié par le règlement (UE) 2019/817 (« Interopérabilité frontières et visas »), la note de bas de page de l'art. 109*a*, al. 1, doit être modifiée en conséquence.

Cette disposition doit en outre être coordonnée avec l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise du règlement (UE) 2018/1240 portant création d'un système européen d'autorisation et d'information concernant les voyages (ETIAS) (développements de l'acquis de Schengen).

Al. 1bis

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

Art. 109b, titre, al. 1, 2, 2bis et 3 et note de bas de page

Le nouveau titre *Système central d'information sur les visas (C-VIS) et système national d'information sur les visas (ORBIS)* de cette section introduit l'abréviation *ORBIS*, qui désigne le système national d'information sur les visas, dans la LEI. En conséquence, dans les dispositions suivantes, *système national d'information sur les visas* est remplacé par *ORBIS*.

36 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

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 actualisée.

Section 6 Système d'information destiné à la mise en œuvre des retours

Une nouvelle section est ajoutée avant l'art. 109*f* LEI. Elle porte sur 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 (Normes procédurales et systèmes d'information) du 14 décembre 2018 ; elles entreront en vigueur début 2020[37]. Aucune modification matérielle n'y a été apportée.

Section 7 Eurodac

Une nouvelle section est ajoutée avant l'art. 109*k*. Elle porte sur les règles concernant Eurodac.

Art. 109k Saisie et transmission de données dans Eurodac

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

Les éléments 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 relatives aux documents de voyage des personnes enregistrées dans Eurodac. Toutefois, le règlement (UE) 2019/818 s'applique à Eurodac à compter de la date d'application de la nouvelle version du règlement (UE) n° 603/2013[38] (art. 75 du règlement [UE] 2019/818).

Art. 109l

Cet article reprend l'actuel article 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 8 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 SEM.

Art. 109m

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

37 FF **2018 7885**
38 JO L 180 du 29.6.2013, p. 1

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

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

Art. 110

L'art. 111 a été abrogé par la modification de la LEI (Normes procédurales et systèmes d'information) du 14 décembre 2018[39]. L'art. 110 réglemente désormais le service partagé pour la comparaison des données biométriques (BMS partagé). L'art. 110 actuellement en vigueur n'est plus nécessaire et est abrogé.

Al. 1 et 3

Le BMS partagé permet de consulter les systèmes d'information Schengen-Dublin concernés par l'interopérabilité des systèmes au moyen de modèles biométriques issus des données biométriques à caractère personnel contenues dans le CIR et le SIS. Ces modèles ne permettent pas d'en déduire les données biométriques réelles.

Le BMS partagé est l'un des quatre nouveaux éléments centraux de l'interopérabilité. Contrairement au CIR (art. 110*a* ss LEI) ou au MID (art. 110*g* LEI), il ne constitue toutefois 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 BMS partagé ne sont pas des données biométriques à caractère personnel ; aucune autre donnée personnelle non plus n'est stockée dans ce système (cf. ch. 3.2.1).

Par souci d'exhaustivité, il convient de prévoir dans la LEI une disposition relative au BMS partagé, et ce, en dépit du fait que les dispositions relatives au BMS partagé des deux règlements de l'UE sur l'interopérabilité sont directement applicables. Les autres nouvelles dispositions de la LEI comportent une référence au BMS partagé.

Le BMS partagé contient des modèles biométriques basés sur des données biométriques à caractère personnel provenant de l'EES, du VIS, d'Eurodac et du SIS. Le système d'information Schengen-Dublin ETIAS ne figure pas sur cette liste, car aucune donnée biométrique à caractère personnel n'y étant stockée.

Al. 2

La référence présente dans le BMS partagé 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 BMS partagé figurent au chapitre III des deux règlements de l'UE sur l'interopérabilité (règlement [UE] 2019/817 et règlement [UE] 2019/818). Le ch. 3.1.2 fournit des informations détaillées sur le BMS partagé.

39 FF **2018 7885**

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

Art. 110a *Contenu du répertoire commun de données d'identité (CIR)*

Al. 1

Pour chaque personne enregistrée dans l'EES, le VIS, l'ETIAS ou, à un stade ultérieur, dans Eurodac, le CIR gère un fichier individuel contenant ses données d'identité, les données relatives à ses documents de voyage et ses données biométriques, extraites de ces systèmes d'information Schengen-Dublin. Les données alphanumériques comprennent les données d'identité de la personne concernée ainsi que les données relatives à ses documents de voyage.

Le CIR est destiné à faciliter l'identification des personnes dont les données sont contenues dans les systèmes d'information Schengen 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 sont régis par les art. 110*b* à 110*d* LEI. À l'avenir, toute consultation du CIR passera en principe par l'ESP (cf. art. 110*e* LEI). D'après les dernières prévisions de la Commission européenne, le CIR devrait entrer en service mi- 2022, tandis que l'ESP ne sera opérationnel qu'en milieu d'année 2023. Il reste à savoir si, jusqu'à ce que les deux éléments centraux soient opérationnels, le CIR pourra également ou non être consulté sans l'ESP pendant une période transitoire. Des informations détaillées sur le CIR figurent au point 3.1.3.

Al. 2

Pour chaque ensemble de données d'identité, de données relatives aux documents de voyage et de données biométriques stockées, le CIR contient une référence au système d'information Schengen-Dublin d'où proviennent les données ainsi qu'une référence à l'ensemble de enregistrements contenus dans le système d'information Schengen-Dublin correspondant. Ces références sont utilisées notamment par une autorité qui n'a pas accès au système d'information Schengen d'où les données sont extraites à l'origine, pour lui permettre de s'adresser à l'autorité centrale compétente afin d'obtenir les données nécessaires.

Les règles détaillées relatives au CIR figurent au chapitre IV des deux règlements de l'UE sur l'interopérabilité (règlement [UE] 2019/817 et règlement [UE] 2019/818).

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

Al. 1 et 2

Conformément à l'art. 20, par. 1, des règlements (UE) 2019/817 et (UE) 2019/818, une consultation peut être menée à des fins d'identification, uniquement dans les circonstances suivantes (par. 1, let. a, et 2):

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

En cas de catastrophe naturelle, d'accident ou d'attentat terroriste, les autorités chargées d'effectuer des recherches dans le système en vertu de l'art. 110*b*, al. 3, LEI 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 énumère les autorités habilitées à mener des recherches dans le CIR, dans des cas particuliers, afin d'identifier des étrangers (ressortissants d'États tiers). Ces autorités sont fedpol, les autorités cantonales et communales de police et de l'Administration fédérale des douanes (AFD), , afin d'assurer la sécurité intérieure et de protéger la population. 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. Une consultation peut en outre être effectuée aux seules fins suivantes : pour lutter contre l'immigration clandestine, pour garantir et maintenir la sécurité et l'ordre publics et pour préserver la sécurité intérieure.

Al. 4 et 5

Les recherches dans le CIR sont généralement effectuées en se fondant sur les données biométriques de l'étranger prélevées directement sur place et à jour. 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 d'identification. Si une recherche au moyen de données bio-

métriques est impossible ou si elle n'aboutit pas, elle doit être effectuée en se fondant sur les données relatives au document de voyage ou les données d'identité disponibles.

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. 3.1.4), 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 relatives aux documents de voyage et à la référence au système d'information Schengen Dublin dont proviennent ces données.

Al. 2

Si un lien rouge apparaît lors d'une recherche dans le CIR (cf. ch. 3.1.4), les autorités ayant accès au CIR, à l'EES, à l'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. commentaires relatifs à l'art. 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'investigation en la matière

Al. 1 et 2

Si, dans un cas particulier, tout porte à croire 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, l'ETIAS ou Eurodac contiennent des données sur la personne concernée. Les autorités de police communales (de Zurich, Lugano, etc.) énumérées dans cet alinéa sont autorisées à consulter ces données du fait qu'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. aussi la réglementation figurant à l'art. 109*a*, al. 3, LEI).

Al. 3

Si une recherche dans le CIR révèle que l'un des systèmes d'information Schengen-Dublin susmentionnés contient des données sur la personne concernée, le CIR affiche aux autorités visées à l'al. 1 la référence correspondante à l'EES, au VIS, à

ETIAS ou à Eurodac. La réponse ne peut être utilisée que pour présenter une demande d'accès au système d'information Schengen-Dublin correspondant.

Al. 4

L'autorité visée à l'al. 2 prend contact avec la centrale d'engagement de fedpol afin de demander un accès complet aux données de l'intéressé dans le système d'information Schengen-Dublin concerné. Si une autorité visée à l'al. 2 renonce à demander un tel accès, malgré une référence, les motifs de cette renonciation sont consignés dans un fichier national traçable.

Section 3 Portail européen de recherche (ESP)

Art. 110e

L'ESP doit être mis en place 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. C'est en qualité d'interface unique qu'il permettra la consultation instantanée des informations nécessaires dans les différents systèmes d'information. Il respectera pleinement les droits d'accès ainsi que les exigences en matière de protection des données.

Sur la base des données d'identité, des données relatives aux documents de voyage et des données biométriques à caractère personnel, l'ESP permettra d'effectuer des recherches simultanément dans l'EES, le VIS, l'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 ss des règlements [UE] 2019/817[40] et [UE] 2019/818[41]).

Une recherche par l'ESP est lancée lorsque:

- 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 déjà autorisées à accéder à l'une des bases de données susmentionnées (art. 7 des règlements [UE] 2019/817[42] et [UE] 2019/818[43]). Afin de permettre l'utilisation de l'ESP, l'agence eu-LISA crée des catégories de profils d'utilisateurs de l'ESP qui

40 Cf. note de bas de page 2
41 Cf. note de bas de page 3
42 Cf. note de bas de page 2
43 Cf. note de bas de page 3

tiennent compte des droits d'accès (art. 8 des règlements [UE] 2019/817[44] et [UE] 2019/818[45]).

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 [UE] 2019/817[46] et [UE] 2019/818[47]. Aucune information n'est fournie sur les données auxquelles l'utilisateur n'est pas autorisé à accéder (art. 9 des règlements [UE] 2019/817[48] et [UE] 2019/818[49].

Chaque État Schengen tient des journaux sur les consultations effectuées dans l'ESP par les autorités compétentes, c'est-à-dire par leur personnel.

La maintenance des interfaces nationales avec les différents systèmes d'information doit permettre de disposer d'autres solutions techniques.

Section 4 Détecteur d'identités multiples (MID)

Art. 110f Contenu du détecteur d'identités multiples (MID)

Le MID est à la fois un détecteur et une nouvelle base de données, à laquelle certaines autorités ont accès. Le MID a pour but de faciliter les contrôles d'identité et de lutter contre la fraude identitaire.

Al. 1

L'al. 1 reprend le contenu de cette base de données, tel que prévu par les règlements de l'UE. Il s'agit des dossiers de confirmation d'identité visés à l'art. 34 des règlements sur l'interopérabilité. C'est également à cette fin que les résultats des recherches sont enregistrés aussi longtemps que les données liées sont stockées dans au moins deux des systèmes Schengen (art. 35 des règlements sur l'interopérabilité).

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 l'ETIAS, ou qu'un signalement est créé ou mis à jour dans le SIS.

44 Cf. note de bas de page 2
45 Cf. note de bas de page 3
46 Cf. note de bas de page 2
47 Cf. note de bas de page 3
48 Cf. note de bas de page 2
49 Cf. note de bas de page 3

Al. 3

L'al. 3 précise comment se déroule un examen des identités multiples dans le cadre de l'interopérabilité des divers systèmes d'information Schengen. Le CIR des systèmes ETIAS, VIS, EES (et plus tard Eurodac) ainsi que le SIS utilisent le BMS partagé (art. 110) et l'ESP (art. 110*e*) lors de la recherche d'identités multiples. Le BMS partagé permet d'effectuer une comparaison biométrique (art. 27, par. 2, des règlements). L'ESP, quant à lui, permet d'effectuer une recherche à l'aide des données d'identité ou des données relatives aux documents de voyage (art. 27, par. 3 et 4, des règlements). 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 le contenu du MID. Il s'agit 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 justifiées ou frauduleuses. Le MID contient également une référence aux systèmes d'information concernés, 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 figurent dans le MID. Le dossier de confirmation d'identité du MID visé à l'art. 34 des règlements (UE) 2019/817 et (UE) 2019/818 contient les éléments suivants:

- le type de lien entre les données, dans la mesure où il existe une concordance (art. 30 à 33 des règlements [UE] 2019/817[50] et [UE] 2019/818[51]);
- une référence aux systèmes d'information Schengen-Dublin dont sont issues les données visées à l'al. 1;
- un numéro d'identification unique;
- l'autorité responsable de la vérification manuelle des différentes identités;
- la date de création du lien ou toute mise à jour de celui-ci.

110g Vérification manuelle de liens 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). Afin de procéder à la vérification manuelle des données, les autorités chargées de la vérification (art. 110*c*) doivent pouvoir accéder au MID. Les autorités compétentes sont identiques à celles pouvant accéder au CIR aux fins de détecter d'éventuelles identités multiples. Il est dès lors fait renvoi à l'art. 110*c*, al. 1, P-LEI, qui désigne les autorités disposant de cet accès au CIR.

50 Cf. notes de bas de page relatives à l'art. 110, al. 1
51 Cf. notes de bas de page relatives à l'art. 110, al. 1

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 actualisant des données dans le C-VIS, l'EES, ou l'ETIAS. Cependant, dans tous les cas où apparaît un lien avec un signalement de nature policière, le bureau SIRENE de fedpol est compétent.

Al. 3

Une vérification des identités multiples a lieu en présence de la personne concernée (art. 29 du règlement [UE] 2019/817). Tel est notamment le cas 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 ne peut s'effectuer en présence de la personne.

Al. 4

Si une identité multiple frauduleuse (lien rouge, art. 32 des règlements 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 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 sur l'interopérabilité). Cette information peut ne pas être communiquée si sa transmission est susceptible d'entrer en conflit avec un signalement figurant dans le SIS ou en cas de nécessité pour des raisons de sécurité et d'ordre publics, pour prévenir la criminalité ou pour garantir qu'aucune investigation nationale ne soit compromise.

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

Art. 110h *Communication de données du BMS partagé, du CIR et du MID*

Par principe, les données des éléments 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 [UE] 2019/817 et 2019/818). Il s'agit de l'article général 111*d* LEI et des articles particuliers 103*d* et 108*f*, qui réglementent la communica-

tion des données des systèmes d'information EES[52] et ETIAS[53]. Les données de ces systèmes peuvent toujours être transmises 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 précis.

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

Cette disposition renvoie à l'art. 40 des deux règlements (UE) 2019/817 et (UE) 2019/818 pour ce qui a trait à la responsabilité du traitement des données des trois éléments d'interopérabilité que sont le BMS partagé, 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

Il convient de renuméroter l'actuel chapitre 14*b* en 14*c*. Ainsi, toutes les dispositions concernant la protection des données dans le cadre des accords d'association à Schengen figureront après le nouveau chapitre 14*b* consacré à l'interopérabilité.

Les dispositions de ce chapitre restent pour l'essentiel inchangées.

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

L'art. 111*d*, al. 5, est abrogé et devient le nouvel art. 109*l* P-LEI.

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

De manière identique, le droit de correction ou d'effacement des données est 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 Schengen et à l'interopérabilité sont ou seront concrétisés dans les ordonnances d'exécution. Pour ce motif, ces divers droits liés à la protection des données ne sont pas mentionnés dans ce chapitre.

52 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, version du JO L 327 du 9.12.2017, p. 20

53 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) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226, version du JO L 236 du 19.9.2018, p. 1

Chapitre 14c Eurodac (actuel)

L'actuel chapitre 14*c*, consacré à Eurodac, est déplacé et apparaît désormais avant le chapitre consacré à l'interopérabilité. Il est ainsi abrogé.

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

L'art. 120*d* en vigueur, adapté dans le cadre des projets EES et ETIAS, doit à nouveau être modifié eu égard à l'interopérabilité. Tout d'abord, le titre de la disposition est modifié et il n'y est plus indiqué qu'il s'agit uniquement de systèmes d'information du SEM. En effet, certains systèmes sont des systèmes Schengen-Dublin, lesquels ne relèvent pas uniquement du SEM.

L'al. 1 est désormais inséré à l'art. 101, al. 2. Il ne subit aucune modification matérielle.

La let. a de l'al. 2 prévoit des sanctions en cas de traitement illicite de données du C-VIS ; la let. b, en cas de traitement illicite de données de l'EES ; la let. c, en cas de traitement illicite de données de l'ETIAS ; une nouvelle let. d, est prévue pour le traitement illicite de données du CIR et une nouvelle let. e, en cas de traitement illicite de données du MID. Tout traitement des données contrevenant aux art 110*a à* 110*d*, 110*f* et 110*g* P-LEI est passible, conformément au code pénal suisse, 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.

Le poursuite pénale relève de la compétence cantonale conformément à l'actuel art. 120*e* LEI.

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*f*.

5.2 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*.

Art. 15 Communication à des destinataires à l'étranger, 111a à 111d

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

5.3 Loi sur la responsabilité

Titre du chapitre Va

Dans la présente loi, 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 donc adapté comme suit: *Chapitre Va Responsabilité des dommages découlant de l'exploitation des systèmes d'information Schengen-Dublin ou de leurs composants.*

Art. 19a

L'actuel art. 19*a* de la LRCF réglemente la responsabilité pour ce qui est du SIS. Il stipule 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 éléments centraux, à l'art. 46 du règlement (UE) 2019/817 et du règlement (UE) 2019/818.

Par conséquent, l'EES (let. b), le VIS (let. c), ETIAS (let. d), le CIR (let. e), l'ESP (let. f), le MID (let. g) et Eurodac (let. h) sont intégrés dans la disposition.

Art. 19b

Le présent article est lui aussi modifié. Il comporte désormais deux alinéas. La formulation "un système d'information Schengen-Dublin ou un de ses composants" remplace la référence au SIS à la let. a. L'actuelle let. b concerne actuellement un dommage en rapport avec un signalement dans le SIS. D'une façon plus générale, et par là en harmonie avec tous les systèmes d'information Schengen-Dublin et leurs composants, il doit y être question de "traitement des données".

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

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

Adaptation de la systématique

Plusieurs articles de la LSIP régissant les systèmes d'information Schengen-Dublin ou leurs composants doivent être complétés, raison pour laquelle la systématique est modifiée. Les systèmes d'information Schengen-Dublin et leurs composants sont dorénavant réglementés dans une section distincte (4), à la suite des systèmes d'information de police "nationaux".

Art. 2

Le présent article liste les systèmes d'information réglementés dans la LSIP. Comme indiqué au ch. 4.3.1, les éléments 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 fédéraux (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. 16) au ch. 3 et le système de gestion des affaires et des documents de fedpol (art. 17) 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. 18) est désormais mentionnée au ch. 1. Les éléments centraux sBMS (régi à l'art. 18*a*), ESP (art. 18*b*) et MID (art. 18*c*) sont ajoutés aux ch. 2 à 4, dans l'ordre de leur mise en service prévue.

Art. 16, 17

Par suite de l'adaptation de la systématique, l'index national de police (actuel art. 17) et le système informatisé de gestion interne des affaires et des dossiers de fedpol (actuel art. 18) sont désormais formellement régis aux art. 16 et 17, avant les systèmes "internationaux".

Nouveau titre: Section 4 Systèmes d'information Schengen-Dublin et leurs composants

Les systèmes d'information Schengen-Dublin et leurs composants étant désormais réglementés dans une section distincte (4), un titre adéquat doit être introduit.

Le SIS, jusqu'ici régi à l'art. 16, trouve à présent sa base légale formelle à l'art. 18.

Art. 18a 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 désormais le cas à l'art. 110 LEI. Malgré une applicabilité directe des deux règlements (UE) 2019/817 et (UE) 2019/818, il est complété par souci d'exhaustivité; il est ainsi plus facile de lui 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 ad hoc du CIR proviennent de l'EES, du VIS et d'Eurodac. C'est ce que précise le présent article.

Al. 2

La référence à l'al. 2 renvoie au système d'information Schengen-Dublin à partir duquel les modèles biométriques ont été initialement 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 des données correspondantes dans le CIR ou dans le SIS entraîne la suppression des données dans le sBMS.

Art. 18b Portail de recherche européen (ESP)

L'ESP doit être réglementé 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, par une seule et même recherche et au moyen des données d'identité, des données relatives aux documents de voyage ou des données biométriques, d'interroger simultanément tous les systèmes d'information Schengen-Dublin pertinents (SIS, EES, VIS, ETIAS, Eurodac et CIR), les bases de données d'Interpol ainsi que les données d'Europol.

Al. 2

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

Al. 3

Les autorités autorisées peuvent consulter les systèmes au moyen des données d'identité, des données relatives aux documents de voyage ou des données biométriques. Elles peuvent rechercher 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 en ligne. Le système d'où proviennent les données ainsi que les liens existants s'affichent également.

Conjointement avec les États Schengen, l'eu-LISA doit encore définir dans un acte d'exécution 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 fixés par voie de règlement.

Al. 5

Il est prévu, sur le plan technique, qu'une "plate-forme nationale de recherche" soit créée pour le raccordement à l'ESP, à laquelle les systèmes d'information de police des cantons seront également reliés, pour autant que les deux règlements européens l'autorisent. Pour l'heure toutefois, on en sait encore trop peu au niveau technique pour qu'une base légale formelle détaillée puisse déjà être prévue. Cette base sera complétée ultérieurement.

Art. 18c Contenu du détecteur d'identités multiples (MID)

Le MID lui aussi concerne le SIS et doit être réglementé dans la LEI (art. 110*f*) comme dans la LSIP (art. 18*c*).

Al. 1

L'al. 1 régit la finalité du MID et son contenu. Le MID 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. C'est le cas par exemple lorsque des données sont saisies ou mises à jour dans le SIS, l'EES, ETIAS, le VIS et, dans l'avenir, Eurodac.

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 déjà enregistrés dans le sBMS. De même, les données d'identité et les données relatives aux documents 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 (UE) 2019/817 et (UE) 2019/818) 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. 18d 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. à ce sujet art. 110, al. 1, LEI).

Al. 1

Les droits d'accès servent à la vérification manuelle des liens jaunes (pour lesquels il n'y a pas encore eu de vérification manuelle).

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'Administration fédérale des douanes (AFD) ou la police cantonale. Si le lien concerne le C-VIS, c'est le SEM ou d'autres autorités chargées des visas et 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 classifier 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. Il est possible d'y renoncer si cette information irait à l'encontre d'un signalement dans le SIS et si c'est nécessaire pour protéger la sécurité et l'ordre public, pour prévenir la criminalité et 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 lorsqu'il s'agit d'un contrôle à l'entrée en Suisse en tant que premier État Schengen.

Art. 18e Communication de données du sBMS, du CIR et du MID

Le présent article régit la communication de données provenant des systèmes d'information Schengen-Dublin et de leurs composants. Les données ne peuvent être transmises à des États tiers, des organisations internationales ou des services privés. Les prescriptions prévues pour chacun des systèmes relatives à la communication des données continuent de s'appliquer.

Art. 18f 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 s'aligne sur l'art. 40 des règlements (UE) 2019/817 et (UE) 2019/818.

6 Conséquences

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

fedpol et le SEM doivent s'attendre à des conséquences financières et sur l'état du personnel, dans la phase de projet comme dans l'application des règlements de l'UE sur l'interopérabilité. Chacune de ces conséquences est détaillée ci-après.

6.1.1 Coûts de projet pour fedpol et le SEM

À fedpol, la mise en œuvre technique et organisationnelle des deux règlements européens sera coordonnée au sein du projet Interopérabilité TO. Principale tâche: le raccordement de la partie nationale du Système d'information Schengen N-SIS aux éléments centraux CIR, MID et ESP. En raison de spécifications techniques manquantes, on ne sait pas à ce jour comment les composants de l'infrastructure nationale devront être adaptés du fait de la vérification de liens MID.

Au SEM, la mise en œuvre des règlements européens se fera dans le cadre du projet Interopérabilité SEM, lequel porte sur des sujets techniques transversaux, comme l'utilisation conjointe de nouveaux composants de système pour les interfaces Schengen, et sur des modifications organisationnelles. De nouveaux processus fondés sur les quatre nouveaux éléments centraux seront sans doute nécessaires et devront être attribués à des unités organisationnelles.

fedpol et le SEM coordonnent sur le plan tant stratégique qu'opérationnel leurs projets visant à la mise en œuvre technique et organisationnelle des règlements de

l'UE sur l'interopérabilité. Afin d'exploiter les synergies entre les projets au niveau opérationnel, des rencontres de coordination auront lieu régulièrement entre les chefs de programme et de projet concernés. L'échange d'informations sera garanti par les contacts directs et un accès réciproque aux plates-formes de projet. L'interopérabilité est un des projets compris dans le programme du GS EJPD « développements de l'acquis Schengen/Dublin ». Dans le cadre de ce programme les projets sont coordonnés en matière du respect des délais, du budget et des exigences de qualité. Un comité directeur stratégique siégeant régulièrement permettra de traiter des questions stratégiques transversales.

Les projets en sont pour l'heure à la phase d'initialisation / de conception. Le raccordement concret aux éléments centraux dépend entre autres de leur conception par l'agence eu-LISA et des particularités techniques. Le développement est prévu au fil de la mise en service échelonnée par l'UE des éléments centraux. Les premiers actes d'exécution de l'UE relatifs à l'interopérabilité sont attendus fin 2019; fedpol et le SEM en sauront alors davantage sur la mise en œuvre. Les coûts de projet actuellement budgétés se fondent sur des estimations de la charge prévisionnelle.

Dans la phase de projet, les conséquences devraient être les suivantes:

Les coûts liés aux projets d'interopérabilité de fedpol et du SEM sont estimés à 21,6 millions de francs pour l'ensemble de la durée du projet, et à 14,1 millions pour les années 2020-2022. Un nouveau crédit d'engagement pour le développement de l'acquis de Schengen et Dublin, crédit d'engagement intégré dans le programme du SG DFJP et approuvé par le Conseil fédéral le 4 septembre 2019, financera le projet. Le programme sera mené comme un projet informatique clé. Les 14,1 millions de francs prévus pour la période 2020-2022 sont compris dans la première tranche du crédit d'engagement et seront couverts par les moyens informatiques centraux alloués par le Conseil fédéral et par des prestations propres des offices concernés.

Coûts Projets Interopérabilité	**Total**	2020	2021	2022	2023	2024	2025
Interopérabilité fedpol	**11,3**	2,9	3,1	1,4	1,5	1,2	1,2
Interopérabilité SEM	**8,3**	2,1	2,2	2,4	1,2	0,2	0,2
Développement IOP (SEM)	**2,0**					1,0	1,0
Total	**21,6**	**5,0**	**5,3**	**3,8**	**2,7**	**2,4**	**2,4**

Ces montants correspondent aux coûts figurant dans le message relatif à un crédit d'engagement pour le développement de l'acquis de Schengen et Dublin, message que le Conseil fédéral a approuvé le 4 septembre 2019.

Pour fedpol, la mise en œuvre de la phase de projet entre 2020 et 2023 devrait occasionner une charge en personnel de 2800 jours-personnes utilisés pour des ressources spécialisées. Le SEM table quant à lui sur 3960 jours-personnes pour la même période. Les moyens en personnel correspondants seront compensés à l'interne. Les ressources nécessaires selon cette estimation ont été communiquées au

Centre de services informatiques (CSI) en août 2019. Elles pourraient encore être adaptées une fois que le CSI aura procédé à une analyse approfondie des exigences.

6.1.2 Coûts d'application, d'exploitation et de développement pour fedpol et pour le SEM

L'interopérabilité permettra aux autorités compétentes de recevoir davantage d'informations. Le nombre de réponses positives et, partant, de cas, augmentera. La sécurité au sein de l'espace Schengen en sera grandement accrue. Mais cette hausse du nombre de cas ira de pair avec une plus grande charge de travail pour les traiter. La vérification de liens MID en vue de l'identification correcte des personnes constituera par ailleurs une nouvelle tâche pour les autorités. C'est pourquoi l'application des règlements sur l'interopérabilité entraînera un besoin accru en personnel autant à fedpol qu'au SEM. Le contrôle de données biométriques induit par la vérification de liens MID surtout s'accompagnera d'une surcharge en personnel au bureau SIRENE, à la Division Identification biométrique de fedpol (BiomID) et dans certains services du SEM. Il n'est pas possible pour l'heure de chiffrer de manière fiable les besoins en personnel, mais ils seront précisés dans le message.

Les coûts d'exploitation supplémentaires à compter de la mise en service de l'interopérabilité de quelque 0,2 million de francs seront couverts par une repriorisation des moyens déjà disponibles. L'éventuelle nécessité de ressources financières et en personnel supplémentaires sera examinée et justifiée lors de la rédaction du message concernant l'approbation et la mise en œuvre des règlements de l'UE sur l'interopérabilité.

Les développements techniques prévues sur les éléments centraux à partir de la mise en œuvre de l'interopérabilité jusqu'à 2025 devraient causer des coûts annuels d'environ un million de francs; ils seront intégrés, après la mise en service des éléments centraux prévue en 2023, dans le projet Développement IOP du SEM (par ex. sur le nœud d'accès national). On ne s'attend pas à des coûts d'exploitation supplémentaires.

6.1.3 Coûts pour l'AFD

Le présent développement aura des conséquences sur les finances, les processus et le personnel de l'AFD. D'une part, des adaptations devront être effectuées sur les interfaces des systèmes existants et d'autre part, d'autres systèmes devront être implémentés, comme l'ESP obligatoire pour les contrôles aux frontières extérieures de Schengen. Les éventuelles adaptations résultant de la création d'une plate-forme nationale de recherche doivent en plus être prises en considération.

L'ESP obligatoire pour le contrôle des personnes aux frontières extérieures de Schengen entraînera des adaptations des processus opérationnels, notamment dans la détection d'identités fausses ou multiples. Dans l'état actuel des choses, on estime que l'économie induite par une plus grande automatisation et les charges induites par la détection des fausses identités devraient plus ou moins se compenser. Les

conséquences sur l'état du personnel se rapportent aux mesures de formation (continue).

La surcharge avec incidences financières pour la direction du projet et la charge de développement pour les adaptations des solutions mobiles et stationnaires de contrôle aux frontières devraient se monter à quelques millions de francs. Selon les informations actuelles, les coûts font partie du programme DaziT de l'AFD. Les obligations financières qui en découlent seront imputées sur le crédit global ad hoc.

6.2 Conséquences techniques

La reprise et la transposition des règlements de l'UE sur l'interopérabilité auront également des conséquences techniques.

Un composant national supplémentaire permettra de raccorder les systèmes suisses à l'ESP. L'interopérabilité des systèmes de police nationaux et cantonaux devrait elle aussi en être améliorée. L'objectif est d'exploiter les synergies entre les systèmes d'information et de présenter les résultats de recherche aux utilisateurs de manière plus claire et plus rapide. fedpol et le SEM collaborent étroitement pour vérifier si cet objectif peut être réalisé au moyen d'une nouvelle plate-forme nationale de recherche, de laquelle les cantons pourraient eux aussi profiter. Une étude préliminaire rédigée à ce sujet dans le cadre de l'harmonisation de l'informatique policière suisse (HiP) en est arrivée à la conclusion que l'utilité et la faisabilité d'une plate-forme nationale de recherche sont évidentes. Elle recommande de centraliser l'exploitation de la plate-forme, mais de maintenir auprès de chaque autorité la conservation des données et l'exploitation des systèmes d'information. Les droits d'accès des autorités ne changeront pas. Ce composant national sera financé par le crédit d'engagement pour le développement de l'acquis de Schengen et Dublin.

6.3 Conséquences pour les cantons et les communes

Les règlements de l'UE sur l'interopérabilité auront des conséquences pour la Confédération, mais aussi pour les autorités cantonales de police et de migration.

Il sera obligatoire d'utiliser l'ESP pour les contrôles aux frontières extérieures de Schengen, raison pour laquelle les autorités de contrôle aux frontières doivent s'attendre à une plus grande charge de travail, notamment dans la deuxième ligne de contrôle. Étant donné que davantage de systèmes d'information seront consultés en même temps, les chances d'une réponse positive sont plus grandes. L'AFD et les autorités de police cantonales chargées du contrôle aux frontières extérieures de Schengen devront vérifier les liens MID, ce qui constitue une nouvelle tâche pour elles et peut, associé aux tâches de suivi, induire une surcharge de travail. D'autres autorités, comme les polices cantonales et les autorités cantonales de migration, pourront toutefois elles aussi utiliser l'ESP. Il est donc prévu que les polices cantonales et communales puissent accéder aux données du CIR pour identifier des personnes se trouvant déjà dans l'espace Schengen, ce qui améliorera l'identification correcte des personnes. Dans leur travail sur les infractions graves et le terrorisme

(prévention, investigation, constatation ou poursuite), les polices cantonales pourront aussi profiter de la nouvelle procédure prévue concernant l'accès des autorités de poursuite pénale, dans la mesure où une consultation du CIR leur permettra de vérifier si des données relatives à une personne figurent dans l'un des systèmes européens. En sa qualité de point d'accès central pour les recherches par les autorités de poursuite pénale dans les systèmes d'information non policiers, fedpol est chargé d'octroyer à ces dernières l'accès aux données nécessaires. Ce processus est déjà appliqué dans le cas du VIS et est prévu pour l'EES.

Les nouveautés de l'interopérabilité induiront probablement des adaptations de diverses applications cantonales. Le raccordement des systèmes suisses à l'ESP par exemple nécessitera des adaptations techniques sur les systèmes de recherche cantonaux. D'autres adaptations sont éventuelles, qu'il n'est pour l'heure pas possible de citer de manière exhaustive.

Les processus opérationnels devront eux aussi probablement être modifiés. La vérification des liens MID constitue une nouvelle tâche pour les autorités concernées. Ces liens sont le résultat du contrôle d'identités multiples effectué pour chaque saisie ou modification de données dans l'un des systèmes européens. Toute vérification nécessaire de données biométriques devra se faire au niveau de fedpol (BioMID). La surcharge de travail qui en découlera est difficile à estimer pour l'instant puisqu'aucun chiffre concret concernant le nombre de liens à attendre n'est encore disponible. Il est également difficile de dire à quel point les cantons seront concernés par ces vérifications, les processus concrets de vérification des liens MID devant encore être clarifiés.

La probable charge de travail supplémentaire doit être mise en regard des grands avantages qu'apporte l'interopérabilité. Au lieu d’interroger les systèmes d’information séparément, l’interopérabilité permettra aux autorités de contrôle aux frontières, de migration et de poursuite pénale d’obtenir une vue d’ensemble des informations existantes sur une personne avec une requête. Les processus opérationnels deviennent donc plus efficaces parce que tous les systèmes ne doivent pas être interrogés individuellement. Le risque que des données restent inaperçues est réduit et la probabilité d’un résultat est augmentée. Les informations disponibles pourront être utilisées de manière plus efficace et ciblée, soit une importante valeur ajoutée pour le travail des autorités de contrôle aux frontières, de migration et de poursuite pénale.

6.4 Conséquences dans d'autres domaines

Il ne devrait pas y avoir de conséquences directes sur l'économie, la société et l'environnement, raison pour laquelle ces questions n'ont pas été examinées en détail. L'interopérabilité accroîtra la sécurité dans l'espace Schengen, ce qui aura une influence positive sur l'économie et la société.

7 Aspects juridiques

7.1 Constitutionnalité

L'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 2019/818 relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE se fonde sur l'art. 54, al. 1, de la Constitution (Cst.)[54], selon lequel 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. Le Conseil fédéral ne peut ici invoquer cette compétence (cf. art. 7*a*, al. 1 et 2, LOGA et art. 24, al. 2, de la loi du 13 décembre 2002 sur le Parlement [LParl][55]). L'approbation des deux échanges de notes incombe donc à l'Assemblée fédérale.

7.2 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'application uniforme des systèmes d'information Schengen et Dublin. La reprise des deux règlements européens et les modifications légales qu'elle induit sont ainsi conformes au droit international.

7.3 Forme de l'acte à adopter

La reprise des deux règlements de l'UE n'étant 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). Et sont 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. ci-dessus ch. 3). Le présent arrêté fédéral est donc soumis au référendum facultatif en vertu de l'art. 141, al. 1, let. d, ch. 3, Cst.

54 RS **101**
55 RS **171.10**

L'Assemblée fédérale approuve les traités internationaux sous la forme d'un arrêté fédéral lorsqu'ils sont soumis 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 légales 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.

7.4 Aspects juridiques particuliers concernant l'acte de mise en œuvre

Délégation de compétence au Conseil fédéral en vertu de l'art. 110h LEI et de l'art. 22 LSIP

Cette délégation de compétence au Conseil fédéral se fonde sur l'art. 182, al. 1, Cst., selon lequel le Conseil fédéral peut édicter des règles de droit sous la forme d'une ordonnance. Il s'agit en l'occurrence de règles de droit nécessaires à la mise en œuvre de la législation de même que des règlements de l'UE sur l'interopérabilité.

Liste des abréviations utilisées

AAS	accord d'association à Schengen
bureau SIRENE	bureau national chargé de la coordination et du traitement de tous les signalements SIS (*Supplementary Information Request at the National Entry*)
CIR	répertoire commun de données d'identité (*Common Identity Repository*)
Commission LIBE	Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (*Civil Liberties, Justice and Home Affairs*)
COREPER	Comité des représentants permanents des États membres
ECRIS-TCN	système européen d'information sur les casiers judiciaires de ressortissants d'États tiers *(European Criminal Records Information System for Third Country Nationals)*
EES	système d'entrée et de sortie (*Entry-Exit System*)
ESP	portail de recherche européen (*European Search Portal*)
ETIAS	système européen d'information et d'autorisation concernant les voyages (*European Travel Information and Authorisation System)*
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 sur les empreintes digitales de requérants d'asile et de personnes appréhendées lors de leur entrée illégale (*European Asylum Dactyloscopy Database*)
HiP	harmonisation de l'informatique policière suisse
IOP	Interopérabilité
IOP Frontières	règlement (UE) 2019/817
IOP Police	règlement (UE) 2019/818

MID	détecteur d'identités multiples (*Multiple Identity Detector*)
sBMS	service partagé d'établissement de correspondances biométriques (*shared Biometric Matching Service*)
SIS	Système d'information Schengen *(Schengen Information System)*
SLTD	base de données d'Interpol sur les documents de voyage volés ou perdus (*Stolen and Lost Travel Documents Database*)
TDAWN	base de données d'Interpol sur les documents de voyage associés aux notices (*Travel Documents Associated with Notices*)
VIS	système d'information sur les visas (*Visa Information System*)