Conseil de
l'Union européenne

Bruxelles, le 2 décembre 2020
(OR. en)

5825/20

IXIM 23
ENFOPOL 41
CT 9
ENFOCUSTOM 25
CRIMORG 14
SCHENGEN 3
VISA 22
SIRIS 18
COPEN 35
ASIM 11
FRONT 22
COMIX 51
JAI 107

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	Groupe de travail sur l'échange d'informations dans le domaine de la JAI (IXIM)
Nº doc. préc.:	9364/19
Objet:	Manuel sur l'échange d'informations en matière répressive

1. Introduction

Le manuel sur l'échange d'informations en matière répressive vise à compléter le manuel des opérations transfrontalières (doc. 10505/4/09 REV 4). Le contenu et la structure du manuel et des fiches nationales ont été approuvés par le groupe DAPIX dans le cadre de la stratégie de gestion de l'information pour la sécurité intérieure de l'UE, en vue de soutenir, de rationaliser et de faciliter l'échange transfrontière d'informations.

Afin d'augmenter l'utilité pratique du manuel, une traduction sera mise à disposition dans chacune des langues officielles de l'Union. En outre, le manuel sera mis à jour deux fois par an, en fonction de la nouvelle législation mise en place ou de l'expérience pratique acquise.

Les coordonnées nationales sont régulièrement mises à jour par les États membres et figurent dans les fiches nationales, qui sont publiées en tant qu'addendum (ADD 1) du manuel. Cet addendum comprend des informations sensibles et ne peut être divulgué sans que le SGC ait été consulté, conformément au règlement (CE) n° 1049/2001[1].

2. Objectif du manuel

Le manuel est essentiellement conçu comme un outil destiné aux fonctionnaires de police qui travaillent dans le domaine de la liaison internationale et, en particulier, aux **opérateurs "PCU"**. Il devrait donc être aussi convivial et complet que possible.

Le manuel a pour but d'éclairer et de faciliter la **coopération pratique au jour le jour** entre les différentes autorités des États membres, qui participent à des échange d'informations de police au niveau à la fois national et international, de servir à des fins de formation et d'assurer la prise de décisions mieux informées lorsqu'il s'agira de rechercher et d'échanger des informations d'un pays à l'autre.

Le manuel contient **un aperçu de l'ensemble des systèmes, des bases juridiques et des instruments d'échange d'informations de l'UE**, qui sont à la disposition des services répressifs des États membres. L'utilisateur est ainsi pleinement informé des possibilités qui existent lorsqu'il s'agit de décider comment rechercher ou fournir des informations d'un pays à l'autre.

Des **fiches nationales** complètent le manuel en spécifiant les coordonnées des points de contact et les informations pouvant faire l'objet d'échanges transfrontières. En actualisant régulièrement ces fiches, les États membres auront satisfait aux nombreuses obligations de notification prévues au titre des différents instruments. Ces fiches nationales devraient faciliter la gestion et l'obtention des informations nécessaires.

Le manuel intègre ces fiches nationales, ainsi que l'essentiel des informations pratiques relatives à la décision-cadre 2006/960/JAI du Conseil ("décision-cadre suédoise"), et il remplace les anciennes lignes directrices concernant la mise en œuvre de la décision-cadre suédoise (doc. 9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

[1] Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission. Ce règlement établit les principes généraux et les limites en matière d'accès.

3. Contenu du manuel

Le manuel est subdivisé en trois parties, qui sont rédigées de manière à pouvoir être consultées séparément les unes des autres, en fonction des intentions du lecteur.

La première partie du manuel consiste en des **listes de points à vérifier** fournissant un aperçu concret des possibilités d'échange d'informations et des aspects pratiques qui y sont relatifs. Ces listes de points à vérifier aident à orienter l'utilisateur vers le point de contact approprié pour l'échange d'informations sur la base de listes de systèmes et de méthodes disponibles dans les grands contextes opérationnels suivants:

– prévention et enquête en matière d'infractions pénales (et d'immigration clandestine);

– lutte contre le terrorisme;

– maintien de l'ordre public et de la sécurité.

En second lieu, une description **générale** présente à la fois les organismes nationaux qui interviennent dans les échanges d'informations et les instruments de ces échanges. Le manuel fait référence au rôle central que jouent la décision-cadre 2006/960/JAI du Conseil ("décision-cadre suédoise") et la décision 2008/615/JAI du Conseil ("décision Prüm") dans le domaine plus large de l'échange d'informations au sein de l'UE. Cependant, le manuel ne se limite pas à ces instruments.

4. Démarche suivie

La rédaction du manuel proposé a été incluse parmi les mesures figurant dans la troisième liste de mesures au titre de la stratégie de gestion de l'information et la première version du manuel a été rédigée au cours des présidences irlandaise, chypriote, grecque, italienne et lettone.

En vue de faciliter davantage l'utilisation du manuel sur l'échange d'informations en matière répressive[2], les délégations sont invitées à diffuser la version actuelle et mise à jour en fonction de leurs besoins.

---

[2] En vertu de l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique, le droit de l'UE concernant l'échange d'informations en matière répressive s'applique au Royaume-Uni et sur son territoire jusqu'à la fin de la période de transition. Après la fin de la période de transition, seul un nombre limité d'actes du droit de l'Union continueront de s'appliquer aux échanges permanents d'informations, selon les conditions prévues dans l'accord.

Conseil de l'Union européenne
Secrétariat général
Direction générale "Justice et affaires intérieures"
Direction "Affaires intérieures"

Manuel sur l'échange d'informations en matière répressive

Sommaire

Introduction 10

PARTIE I - Contexte opérationnel 12

LISTE DE POINTS À VÉRIFIER A: ÉCHANGE D'INFORMATIONS AUX FINS DE PRÉVENTION ET D'ENQUÊTE EN MATIÈRE D'INFRACTIONS PÉNALES 13

LISTE DE POINTS À VÉRIFIER B: ÉCHANGE D'INFORMATIONS AUX FINS DE LUTTE CONTRE LES INFRACTIONS TERRORISTES 22

LISTE DE POINTS À VÉRIFIER C: ÉCHANGE D'INFORMATIONS AUX FINS DE MAINTIEN DE L'ORDRE PUBLIC ET DE LA SÉCURITÉ 32

PARTIE II - INFORMATIONS D'ORDRE GÉNÉRAL 36

1. CANAUX DE CONTACT 37

1.1. PCU - Point de contact unique 37

1.2. Bureaux SIRENE 41

1.3. Unité nationale Europol (UNE) 42

1.4. Bureaux centraux nationaux d'INTERPOL (BCN) 43

1.5. Points de contact nationaux Prüm 44

1.5.1. PCN Prüm - ADN et empreintes digitales 44

1.5.2. PCN Prüm - Données d'immatriculation des véhicules (DIV) 46

1.5.3. PCN Prüm en matière de prévention du terrorisme 47

1.5.4. PCN Prüm en matière d'événements majeurs 47

1.6. Points nationaux (policiers) d'information "football" (PNIF) 48

1.6.1. Manuel concernant les matchs de football 49

1.7. Points focaux nationaux sur les armes à feu 50

1.7.1. Guide sur les bonnes pratiques concernant les points focaux nationaux sur les armes à feu 51

1.8. Centres de coopération policière et douanière (CCPD) 52

1.9. Officiers de liaison 54

1.10. Bureaux de recouvrement des avoirs (BRA) des États membres 55

1.11. Blanchiment de capitaux - Coopération entre cellules de renseignement financier CRF) 57

1.12. Convention Naples II 58

1.13. Unité d'informations passagers (UIP) 59

1.14. Points d'accès nationaux à l'EES 62

1.15. Unités nationales ETIAS 64

1.16. Interopérabilité 67

1.17. Choix du canal - Critères communément utilisés 70

2. SYSTEMES D'INFORMATION 71

2.1. Système d'information Schengen – Deuxième génération (SIS II) 71

2.2. SIE - Système d'information Europol 74

2.3. SIENA - Application de réseau d'échange sécurisé d'informations d'Europol 76

2.4. I-24/7 - Système mondial de communication policière d'Interpol 77

2.4.1. Interpol: Passerelle ADN 77

2.4.2. Base de données d'empreintes digitales d'Interpol 78

2.4.3. Base de données d'Interpol sur les documents de voyage volés ou perdus 78

2.4.4. Documents de voyage associés aux notices (TDAWN) 78

2.4.5. Tableau de référence des armes à feu 78

2.5. ECRIS 79

2.5.1. ECRIS-TCN 80

2.6. Système d'information sur les visas (VIS) 82

2.7. Eurodac 84

2.8. SID – Système d'information douanier 87

2.9. Faux documents et documents authentiques en ligne - FADO 88

2.10. Registre public en ligne des documents authentiques d'identité et de voyage - PRADO 89

2.11. Système d'entrée/de sortie (EES) 89

2.12. Système européen d'information et d'autorisation concernant les voyages (ETIAS) 92

2.13. Tableau synthétique des systèmes d'information utilisés pour l'échange d'information dans l'UE 95

3. LEGISLATION - CONTEXTE JURIDIQUE, REGLES ET ORIENTATIONS RELATIFS AUX PRINCIPAUX MODES ET SYSTEMES DE COMMUNICATION 103

3.1. Directive sur la protection des données 103

3.2. Décision-cadre suédoise 106

3.3. Accord de Schengen 117

3.3.1. Échange de données dans le cadre et en dehors du SIS II 117

3.3.2. Refonte du système d'information Schengen 121

3.4. Europol 123

3.5. Agence européenne de garde-frontières et de garde-côtes (Frontex) 124

3.6. Interpol 127

3.7. Officiers de liaison 128

3.8. Échange de données Prüm 130

3.9. Système d'information sur les visas (VIS) 131

3.10. Eurodac 133

3.11. Naples II 134

3.11.1. Système d'information douanier - SID 135

3.12. Bureaux de recouvrement des avoirs (BRA) et réseau CARIN 136

3.13. Cellules de renseignement financier (CRF) 138

3.14. Accord UE/États-Unis sur le programme de surveillance du financement du terrorisme (TFTP) 141

3.15. Échange d'information sur les casiers judiciaires (ECRIS) 142

3.15.1. Échange d'informations sur les casiers judiciaires des ressortissants de pays tiers et des apatrides (ECRIS-TCN) 144

3.16. Conservation des données de télécommunications 145

3.17. Directive PNR (dossiers passagers) 146

3.18. Informations préalables sur les passagers (données API) 149

3.19. Infractions en matière de sécurité routière 150

3.20. Système d'entrée/de sortie (EES) 151

3.21. Système européen d'information et d'autorisation concernant les voyages (ETIAS) 154

3.22. Législation relative à l'interopérabilité 156

INTRODUCTION

Objectif du présent manuel

La coopération policière transfrontière au sein de l'Union européenne s'appuie fortement sur l'échange d'informations. Le présent manuel vise à faciliter la coopération au jour le jour à cet égard. Il est principalement destiné au PCU national, le point de contact unique chargé de gérer le flux d'informations qui transite entre différentes unités et points de contact désignés, tant au niveau national que sur le plan international.

Le paysage de la coopération européenne en matière répressive[3] se caractérise par une augmentation et une accélération des échanges d'informations. Cela est favorisé, d'une part, par des technologies de l'information et de la communication en constante évolution. Mais, il y a aussi, d'autre part, une multitude de bases de données, à la fois nationales et internationales.

Le présent manuel vise à répondre à la nécessité de trouver le point de contact ou la base de données appropriés dans un contexte opérationnel spécifique. Il expose brièvement quelles sont les législations pertinentes, sans toutefois perdre de vue son but principal, à savoir faciliter l'échange transfrontière d'informations.

Structure du manuel

Le manuel est structuré comme suit:

PARTIE I - "Contexte opérationnel" - partie contenant une série de tableaux ou "listes de points à vérifier" correspondant aux informations figurant dans la *PARTIE II* et la *PARTIE III* et comportant soit la base juridique pertinente soit des informations relatives aux points de contact. Ces listes de points à vérifier se répartissent entre les trois grands domaines thématiques suivants:

- **Prévention de la criminalité (et de l'immigration clandestine) et lutte contre celle(s)-ci - Liste de points à vérifier A**
- **Lutte contre les infractions terroristes - Liste de points à vérifier B**
- **Maintien de l'ordre public - Liste de points à vérifier C**

[3] Aux fins du présent manuel, on entend par "en matière répressive" la prévention et la détection des infractions terroristes, telles qu'elles sont définies dans la directive (UE) 2017/541, ainsi que les enquêtes en la matière, ou les infractions pénales graves, telles qu'elles sont définies à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI relative au mandat d'arrêt européen.

L'objectif de ces listes de points à vérifier est de guider le lecteur du point choisi comme canal ou mode de communication dans un contexte opérationnel spécifique à la source des informations de contact ou tout autre élément approprié en termes de législation, de règles, de réglementations et de manuels de bonnes pratiques.

PARTIE II - "Informations d'ordre général" - partie fixant le paysage en matière répressive en fonction des différents modes et canaux de communication dont disposent les forces de police dans l'UE. Cette deuxième partie se subdivise elle-même en trois domaines qui couvrent les aspects suivants:

- **Canaux de communication (c'est-à-dire organismes qui participent à l'échange d'informations en matière répressive)**

- **Systèmes d'information et bases de données utilisés pour l'échange transfrontière d'informations**

- **Législation - contexte législatif, ainsi que règles et orientations, relatifs aux principaux modes et systèmes de communication**

PARTIE III - "Fiches nationales" - partie, disponible dans l'addendum 1 de la présente note, contenant des fiches nationales où figurent des informations détaillées sur les points de contact pertinents pour tous les aspects de l'échange transfrontière d'informations mentionnées dans l'ensemble du document. Il appartient aux États membres de notifier toute modification au Secrétariat général du Conseil dans les plus brefs délais. En actualisant régulièrement les fiches nationales dans l'addendum du manuel, les États membres auront respecté leurs nombreuses obligations de notification prévues au titre des différents instruments. Il devrait ainsi être plus facile de gérer et de trouver ces informations à l'avenir.

PARTIE I - CONTEXTE OPERATIONNEL

LISTE DE POINTS À VÉRIFIER A: ÉCHANGE D'INFORMATIONS AUX FINS DE PRÉVENTION ET D'ENQUÊTE EN MATIÈRE D'INFRACTIONS PÉNALES

Système d'information	Point d'accès national	Base juridique	Manuel
Système d'information Schengen / SIS II	SIRENE (Bureau "Supplément d'information requis à l'entrée nationale")	Acquis de Schengen visé à l'article 1er, paragraphe 2, de la décision 1999/435/CE du Conseil du 20 mai 1999 JO L 239 du 22.9.2000, p. 1 Règlement (CE) n° 1987/2006 JO L 381 du 28.12.2006, p. 4 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).	Version révisée du catalogue mis à jour de recommandations pour l'application correcte de l'acquis de Schengen et de meilleures pratiques Doc. 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Décision d'exécution (UE) 2017/1528 de la Commission remplaçant l'annexe de la décision d'exécution 2013/115/UE relative au manuel Sirene et à d'autres mesures d'application pour le système d'information Schengen de deuxième génération (SIS II) (JO L 231 du 7.9.2017, p. 6).

Europol / Système d'information Europol - Système d'index SIE Fichiers de travail à des fins d'analyse - FTA	UNE	Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à partir du 1er mai 2017)	
Interpol / I-24/7	BCN (Bureau central national)	Règlement d'INTERPOL sur le traitement des données [III/IRPD/GA/2011(2014)] Règlement relatif au contrôle des informations et à l'accès aux fichiers d'INTERPOL [II.E/RCIA/GA/2004(2009)]	
ADN / PRÜM - Consultation automatisée de bases de données nationales désignées	Point de contact national 1re étape: consultation automatisée	Décision du Conseil 2008/615/JAI, articles 3 et 4, JO L 210 du 6.8.2008, p. 1	
	2e étape: transmission d'autres données à caractère personnel et d'autres informations	Législation nationale Décision-cadre 2006/960/JAI du Conseil (décision-cadre suédoise) JO L 386 du 29.12.2006, p. 89 Rectificatif, JO L 75 du 15.3.2007, p. 26	

Empreintes digitales / PRÜM - Consultation automatisée de bases de données nationales désignées	Point de contact national 1re étape: consultation automatisée	Décision 2008/615/JAI du Conseil, article 9 JO L 210 du 6.8.2008, p. 1	
	2e étape: transmission d'autres données à caractère personnel et d'autres informations	Législation nationale Décision-cadre 2006/960/JAI du Conseil (décision-cadre suédoise)	
Données relatives à l'immatriculation des véhicules / PRÜM - Consultation automatisée de bases de données relatives à l'immatriculation des véhicules (DIV)	Point de contact national pour les demandes entrantes	Décision 2008/615/JAI du Conseil, article 12 JO L 210 du 6.8.2008, p. 1	
	pour les réponses sortantes	comme ci-dessus	
Données des dossiers passagers (PNR)	Unité d'informations passagers (UIP)	Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière JO L 119 du 4.5.2016, p. 132	

Système d'information sur les visas / VIS	Points d'accès nationaux centraux	Décision 2004/512/CE du Conseil JO L 213 du 15.6.2004, p. 5 Décision 2008/633/JAI du Conseil JO L 218 du 13.8.2008, p. 126 Règlement (CE) n° 767/2008 *JO L 218 du 13.8.2008, p. 60*. Liste des autorités compétentes dont le personnel dûment autorisé sera habilité à saisir, à modifier, à effacer ou à consulter des données dans le système d'information sur les visas (VIS), (2016/C 187/04), JO C 187 du 26.5.2016, p. 4.	

Eurodac	Autorités nationales compétentes	Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte) JO L 180 du 29.6.2013, p. 1 Règlement (UE) n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride JO L 180 du 29.6.2013, p. 31	

SID – Système d'information douanier	Points d'accès nationaux	Décision 2009/917/JAI du Conseil sur l'emploi de l'informatique dans le domaine des douanes JO L 323 du 10.12.2009, p. 20	
Système européen d'information sur les casiers judiciaires / ECRIS	Autorité centrale nationale	Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil JO L 151 du 7.6.2019, p. 143	ECRIS - Manuel non contraignant à l'intention des praticiens disponible au format électronique sur le site du CIRCABC https://circabc.europa.eu
Réseau Camden regroupant les autorités compétentes en matière de recouvrement d'avoirs (CARIN)	Bureaux de recouvrement des avoirs (BRA)	Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime JO L 332 du 18.12.2007, p. 103	Manuel des bonnes pratiques en matière de lutte contre la criminalité financière: une série de bons exemples de systèmes élaborés, mis sur pied dans les États membres pour lutter contre la criminalité financière Doc. 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

CRF.NET	Cellules de renseignement financier (CRF)	Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission JO L 141 du 5.6.2015, p. 73 Les CRF sont également régies depuis peu par la directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil JO L 186 du 11.7.2019, p. 122	Manuel des bonnes pratiques en matière de lutte contre la criminalité financière: une série de bons exemples de systèmes élaborés, mis sur pied dans les États membres pour lutter contre la criminalité financière Doc. 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37

Réseau des points focaux nationaux sur les armes à feu	POINTS FOCAUX NATIONAUX SUR LES ARMES À FEU	Communication de la Commission au Parlement européen et au Conseil (COM(2015) 624 final)) relative à la mise en œuvre du programme européen en matière de sécurité: plan d'action de l'UE contre le trafic et l'utilisation illicite d'armes à feu et d'explosifs. 14971/15 COSI 184 ENFOPOL 404 ENFOCUSTOM 142 CYBER 125 CRIMORG 129 Communication conjointe au Parlement européen et au Conseil. JOIN (2018) 17 final. Éléments à considérer en vue d'une stratégie de l'UE contre les armes à feu, les armes légères et de petit calibre illicites et leurs munitions "Sécuriser les armes, protéger les citoyens" 11271/18 CF SP/PESC 735 CONOP 70 CODUN 26 COARM 218 Conclusions du Conseil sur l'adoption d'une stratégie de l'UE contre les armes à feu et armes légères et de petit calibre illicites et leurs munitions. 13581/18 CONOP 98 CODUN 36 COARM 289 CF SP/PESC 985 COSI 288 ENFOPOL 565	Réseaux et groupes d'experts liés au groupe "Application de la loi" (LEWP) et au groupe d'experts européens en armes à feu (EFE). "Best practice Guidance for the Creation of National Firearms Focal Points" (guide sur les bonnes pratiques en vue de la mise en place de points focaux nationaux sur les armes à feu) 8586/18 ENFOPOL 207

		Directive d'exécution (UE) 2019/69 de la Commission du 16 janvier 2019 établissant des spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes JO L 15 du 17.1.2019, p. 22, article 3 Règlement délégué (UE) 2019/686 de la Commission du 16 janvier 2019 établissant les modalités détaillées, au titre de la directive 91/477/CEE du Conseil, de l'échange systématique, par voie électronique, d'informations relatives au transfert d'armes à feu au sein de l'Union JO L 116 du 3.5.2019, p. 1, article 3	

LISTE DE POINTS À VÉRIFIER B: ÉCHANGE D'INFORMATIONS AUX FINS DE LUTTE CONTRE LES INFRACTIONS TERRORISTES

Système d'information	Point d'accès national	Base juridique	Manuel
Système d'information Schengen / SIS II	SIRENE (Bureau "Supplément d'information requis à l'entrée nationale")	Acquis de Schengen visé à l'article 1er, paragraphe 2, de la décision 1999/435/CE du Conseil du 20 mai 1999 JO L 239 du 22.9.2000, p. 1 Règlement (CE) n° 1987/2006 JO L 381 du 28.12.2006, p. 4 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).	Version révisée du catalogue mis à jour de recommandations pour l'application correcte de l'acquis de Schengen et de meilleures pratiques Doc. 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484 Décision d'exécution (UE) 2015/219 de la Commission du 29 janvier 2015 remplaçant l'annexe de la décision d'exécution 2013/115/UE relative au manuel SIRENE et à d'autres mesures d'application pour le système d'information Schengen de deuxième génération (SIS II) [notifiée sous le numéro C(2015) 326]

Europol / Système d'information Europol - Système d'index SIE Fichiers de travail à des fins d'analyse - FTA	UNE	Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à partir du 1er mai 2017)	
Interpol / I-24/7	BCN (Bureau central national)	Règlement d'INTERPOL sur le traitement des données [III/IRPD/GA/2011(2014)] Règlement relatif au contrôle des informations et à l'accès aux fichiers d'INTERPOL [II.E/RCIA/GA/2004(2009)]	
ADN / PRÜM - Consultation automatisée de bases de données nationales désignées	Point de contact national 1re étape: consultation automatisée	Décision du Conseil 2008/615/JAI, articles 3 et 4, JO L 210 du 6.8.2008, p. 1	
	2e étape: transmission d'autres données à caractère personnel et d'autres informations	Législation nationale Décision-cadre 2006/960/JAI du Conseil (décision-cadre suédoise) JO L 386 du 29.12.2006, p. 89 Rectificatif, JO L 75 du 15.3.2007, p. 26	

Empreintes digitales / PRÜM - Consultation automatisée de bases de données nationales désignées	Point de contact national 1re étape: consultation automatisée	Décision 2008/615/JAI du Conseil, article 9 JO L 210 du 6.8.2008, p. 1	
	2e étape: transmission d'autres données à caractère personnel et d'autres informations	Législation nationale Décision-cadre 2006/960/JAI du Conseil (décision-cadre suédoise)	
Données relatives à l'immatriculation des véhicules / PRÜM - Consultation automatisée de bases de données relatives à l'immatriculation des véhicules (DIV)	Point de contact national pour les demandes entrantes	Décision 2008/615/JAI du Conseil, article 12 JO L 210 du 6.8.2008, p. 1	
	pour les réponses sortantes	comme ci-dessus	
ADN / PRÜM - Consultation automatisée de bases de données nationales désignées	Point de contact national 1re étape: consultation automatisée	Décision du Conseil 2008/615/JAI, articles 3 et 4, JO L 210 du 6.8.2008, p. 1	*Guide de mise en œuvre - Échange de données ADN* Doc. 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61
Réseau PRÜM pour la transmission de données à caractère personnel ainsi que d'informations spécifiées aux fins de la prévention des infractions terroristes	Point de contact national Prüm en matière de lutte contre le terrorisme	Décision 2008/615/JAI du Conseil, article 16 JO L 210 du 6.8.2008, p. 1	

Données des dossiers passagers (PNR)	Unité d'informations passagers (UIP)	Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière JO L 119 du 4.5.2016, p. 132	
Système d'information sur les visas / VIS	Points d'accès nationaux centraux	Décision 2004/512/CE du Conseil JO L 213 du 15.6.2004, p. 5 Décision 2008/633/JAI du Conseil JO L 218 du 13.8.2008, p. 126 Règlement (CE) n° 767/2008 JO L 218 du 13.8.2008, p. 60 Liste des autorités compétentes dont le personnel dûment autorisé sera habilité à saisir, à modifier, à effacer ou à consulter des données dans le système d'information sur les visas (VIS), (2016/C 187/04), JO C 187 du 26.5.2016, p. 4.	

Eurodac	Autorités nationales compétentes	Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte) JO L 180 du 29.6.2013, p. 1 Règlement (UE) n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride JO L 180 du 29.6.2013, p. 31	

Système européen d'information sur les casiers judiciaires / ECRIS	Autorité centrale nationale	Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil JO L 151 du 7.6.2019, p. 143	ECRIS - Manuel non contraignant à l'intention des praticiens disponible au format électronique sur le site du CIRCABC https://circabc.europa.eu

Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers et les apatrides (ECRIS-TCN)	Autorité centrale nationale	Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 JO L 135 du 22.5.2019, p. 1 Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil JO L 151 du 7.6.2019, p. 143	
Réseau Camden regroupant les autorités compétentes en matière de recouvrement d'avoirs (CARIN)	Bureaux de recouvrement des avoirs (BRA)	Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime JO L 332 du 18.12.2007, p. 103	

CRF.NET	Cellules de renseignement financier (CRF)	Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission JO L 141 du 5.6.2015, p. 73 Les CRF sont également régies depuis peu par la directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil JO L 186 du 11.7.2019, p. 122	

Réseau des points focaux nationaux sur les armes à feu	POINTS FOCAUX NATIONAUX SUR LES ARMES À FEU	Communication de la Commission au Parlement européen et au Conseil (COM(2015) 624 final)) relative à la mise en œuvre du programme européen en matière de sécurité: plan d'action de l'UE contre le trafic et l'utilisation illicite d'armes à feu et d'explosifs. 14971/15 Communication conjointe au Parlement européen et au Conseil. JOIN (2018) 17 final. Éléments à considérer en vue d'une stratégie de l'UE contre les armes à feu, les armes légères et de petit calibre illicites et leurs munitions "Sécuriser les armes, protéger les citoyens" 11271/18 Conclusions du Conseil sur l'adoption d'une stratégie de l'UE contre les armes à feu et armes légères et de petit calibre illicites et leurs munitions. 13581/18 Directive d'exécution (UE) 2019/69 de la Commission du 16 janvier 2019 établissant des spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes JO L 15 du 17.1.2019, p. 22, article 3	Réseaux et groupes d'experts liés au groupe "Application de la loi" (LEWP) et au groupe d'experts européens en armes à feu (EFE). "Best practice Guidance for the Creation of National Firearms Focal Points" (guide sur les bonnes pratiques en vue de la mise en place de points focaux nationaux sur les armes à feu) 8586/18 ENFOPOL 207

		Règlement délégué (UE) 2019/686 de la Commission du 16 janvier 2019 établissant les modalités détaillées, au titre de la directive 91/477/CEE du Conseil, de l'échange systématique, par voie électronique, d'informations relatives au transfert d'armes à feu au sein de l'Union JO L 116 du 3.5.2019, p. 1, article 3	

LISTE DE POINTS À VÉRIFIER C: ÉCHANGE D'INFORMATIONS AUX FINS DE MAINTIEN DE L'ORDRE PUBLIC ET DE LA SÉCURITÉ

Système d'information	**Point d'accès national**	**Base juridique**	
Réseau des points de contact permanents dans le domaine de l'ordre public	Points de contact nationaux	Action commune 97/339/JAI du 26 mai 1997 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la coopération dans le domaine de l'ordre et de la sécurité publics, article 3, point b) JO L 147 du 5.6.1997, p. 1	
Réseau PRÜM pour la transmission de données à caractère personnel ou non aux fins de la prévention des infractions pénales et du maintien de l'ordre et de la sécurité publics lors de manifestations de grande envergure à dimension transfrontière	Point de contact national Prüm / Événements majeurs	Décision 2008/615/JAI du Conseil, article 15 JO L 210 du 6.8.2008, p. 1 Législation nationale	

Réseau des points nationaux d'information "football"	Points nationaux d'information "football" / PNIF	Décision 2002/348/JAI du Conseil du 25 avril 2002 concernant la sécurité lors de matches de football revêtant une dimension internationale JO L 121 du 8.5.2002, p. 1 Décision 2007/412/JAI du Conseil du 12 juin 2007 modifiant la décision 2002/348/JAI concernant la sécurité lors de matches de football revêtant une dimension internationale JO L 155 du 15.6.2007, p. 76	Recommandation 2007/C 314/07 du Conseil du 6 décembre 2007 relative à un Manuel destiné aux autorités de police et de sécurité concernant la coopération lors d'événements majeurs revêtant une dimension internationale JO L 314 du 22.12.2007, p. 4 Résolution du Conseil concernant un manuel actualisé assorti de recommandations pour la mise en place, à l'échelle internationale, d'une coopération policière et de mesures visant à prévenir et à maîtriser la violence et les troubles liés aux matchs de football revêtant une dimension internationale qui concernent au moins un État membre ("manuel de l'Union européenne concernant les matchs de football") JO C 444 du 29.11.2016, p. 1

Réseau des points focaux nationaux sur les armes à feu	POINTS FOCAUX NATIONAUX SUR LES ARMES À FEU	Communication de la Commission au Parlement européen et au Conseil (COM(2015) 624 final)) relative à la mise en œuvre du programme européen en matière de sécurité: plan d'action de l'UE contre le trafic et l'utilisation illicite d'armes à feu et d'explosifs. 14971/15 Communication conjointe au Parlement européen et au Conseil. JOIN (2018) 17 final. Éléments à considérer en vue d'une stratégie de l'UE contre les armes à feu, les armes légères et de petit calibre illicites et leurs munitions "Sécuriser les armes, protéger les citoyens" 11271/18 Conclusions du Conseil sur l'adoption d'une stratégie de l'UE contre les armes à feu et armes légères et de petit calibre illicites et leurs munitions. 13581/18 Directive d'exécution (UE) 2019/69 de la Commission du 16 janvier 2019 établissant des spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes, JO L 15 du 17.1.2019, p. 22, article 3	Réseaux et groupes d'experts liés au groupe "Application de la loi" (LEWP) et au groupe d'experts européens en armes à feu (EFE). "Best practice Guidance for the Creation of National Firearms Focal Points" (guide sur les bonnes pratiques en vue de la mise en place de points focaux nationaux sur les armes à feu) 8586/18 ENFOPOL 207

		Règlement délégué (UE) 2019/686 de la Commission du 16 janvier 2019 établissant les modalités détaillées, au titre de la directive 91/477/CEE du Conseil, de l'échange systématique, par voie électronique, d'informations relatives au transfert d'armes à feu au sein de l'Union JO L 116 du 3.5.2019, p. 1, article 3	
Réseau de protection des personnalités	Points d'accès nationaux	Décision 2009/796/JAI du Conseil du 4 juin 2009 modifiant la décision 2002/956/JAI relative à la création d'un réseau européen de protection des personnalités JO L 283 du 30.10.2009, p. 62	Manuel du réseau européen de protection des personnalités Doc. 10478/13 ENFOPOL 173
Centres de coopération policière et douanière	CCPD	Accords bilatéraux	

PARTIE II - INFORMATIONS D'ORDRE GÉNÉRAL

1. CANAUX DE CONTACT[4]

1.1. PCU - Point de contact unique

De nombreux points de contact nationaux

Les États membres, aussi bien requis que requérants, font face à un flux croissant d'informations transfrontières en améliorant l'efficacité des structures et réseaux opérationnels, tant au niveau national que sur le plan européen. De nombreux instruments juridiques de l'UE dans le domaine de la coopération transfrontière en matière répressive supposent l'établissement d'autorités, d'organismes ou de bureaux compétents particuliers, ou de points de contact nationaux (PCN). La police, les douanes ou les autres autorités compétentes autorisées par la législation nationale doivent s'échanger des informations par l'intermédiaire de ces points de contact nationaux (PCN) désignés qui, au sein d'un État membre donné, peuvent dépendre de différents services au sein des forces de police ou même de différents ministères. Afin de donner une vue d'ensemble, des listes de points de contact nationaux spécifiques pour l'échange d'informations au niveau de l'UE dans le domaine de l'échange de données en matière répressives sont présentées dans la partie III du présent document et sont régulièrement publiées et actualisées par le SGC.

Principe de disponibilité - Décision-cadre suédoise

L'échange d'informations et de renseignements présentant une dimension transfrontière en matière répressive[5] devrait respecter les conditions qui découlent du "principe de disponibilité" mis en œuvre par la "décision-cadre suédoise". Cela signifie:

- que tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre,

- que les services répressifs de l'autre État membre qui détient ces informations les mettront à sa disposition aux fins indiquées, en tenant compte des exigences des enquêtes en cours dans cet autre État, et

---

4 Organismes nationaux participant à l'échange d'informations en matière répressive.

5 Aux fins du présent manuel, on entend par "en matière répressive" la prévention et la détection des infractions terroristes, telles qu'elles sont définies dans la directive (UE) 2017/541, ainsi que les enquêtes en la matière, ou les infractions pénales graves, telles qu'elles sont définies à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI relative au mandat d'arrêt européen, lorsque ces infractions sont punies, en vertu du droit national, d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans.

- que, dès que des informations policières sont disponibles dans un État membre, elles peuvent être partagées au-delà des frontières dans les mêmes conditions qui régissent le partage des informations au niveau national, ce qui signifie que les règles appliquées dans le cadre d'une affaire transfrontière ne sont pas plus strictes que celles qui s'appliquent aux échanges de données au niveau national ("principe d'accès équivalent").

Point de contact unique (PCU)

La combinaison des exigences strictes de la décision-cadre suédoise et l'existence de différentes stratégies nationales visant à gérer les différentes initiatives d'échange d'informations impose une approche plus simple et uniforme au niveau des États membres afin de veiller à ce que toutes les demandes d'informations soumises entre services répressifs dans l'UE soient traitées efficacement et de manière effective.

Les conclusions du Conseil sur le modèle européen d'échange d'informations (EIXM)[6], adoptées en juin 2013, ont reconnu le potentiel d'un point de contact unique en matière d'échange d'informations au sein de chaque État membre lorsqu'il s'agit d'aider à rationaliser le processus dans un environnement juridique et opérationnel de plus en plus complexe.

La politique consistant à effectuer autant d'échange d'informations que possible par l'intermédiaire d'un point de contact unique a été mis en œuvre dans presque tous les États membres, même si la compréhension de ce qui définit un PCU semble varier selon les États membres. Les lignes directrices concernant un PCU[7] indiquent comment les PCU peuvent être structurés afin d'optimiser l'utilisation de ressources, d'éviter les doubles emplois et de rendre la coopération avec les autres États membres plus efficace, plus utile et plus transparente.

À partir de ces lignes directrices, les États membres devraient sélectionner la solution adaptée à leur situation compte tenu de l'objectif commun dont ils sont convenus visant à renforcer la coopération internationale, et envisager des modes d'information appropriés des autres États membres sur la solution choisie en vue de l'échange des meilleures pratiques.

---

6 Conclusions du Conseil faisant suite à la communication de la Commission sur le modèle européen d'échange d'informations (EIXM), doc. 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

7 "Projet de lignes directrices concernant un point de contact unique (PCU) pour l'échange international d'informations en matière répressive", doc. 10492/14 DAPIX 75 ENFOPOL 157 et 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Idéalement, le PCU:

- a accès à l'éventail le plus large possible en matière de bases de données nationales, européenne et internationales pertinentes en matière répressive, afin de pouvoir gérer de manière rapide l'échange direct d'informations entre les autorités nationales compétentes;

- abrite les entités nationales SIRENE, Europol et Interpol;

- abrite le point de contact pour les officiers de liaison, les points de contact désignés au titre de la décision-cadre suédoise et des "décisions Prüm" et, le cas échéant, les points de contact pour les bureaux régionaux et bilatéraux;

- est mis en place dans un environnement de travail sécurisé et est doté d'un personnel suffisant et compétent, y compris de moyens d'interprétation ou de traduction, pour fonctionner 24 heures sur 24 et 7 jours sur 7. Dans la mesure du possible, tout le personnel devrait être formé et équipé/mandaté pour traiter tous les types de tâches au sein du PCU. Lorsque cela n'est pas possible, il convient de veiller à ce que toutes les tâches puissent être accomplies par des agents de garde 24 heures sur 24 et 7 jours sur 7;

- est une organisation regroupant de multiples agences, dont le personnel provient ou relève de différents services et/ou ministères, notamment la police judiciaire, les gardes-frontières, les douanes et les autorités judiciaires.

Structure typique d'un bureau national PCU (point de contact unique)

Unité centrale de coopération policière opérationnelle,

Plateforme d'échange d'informations

La Section centrale de coopération opérationnelle de police (SCCOPOL) est une structure ***interministérielle*** *composée de 67 policiers, gendarmes et agents des douanes. Les magistrats du bureau de l'entraide pénale internationale (BEPI) du ministère de la justice accueille également, dans les mêmes locaux, un service de base visant à valider les demandes françaises d'émission de mandats d'arrêt européens et d'enregistrement, dans le fichier national des personnes recherchés, de demandes d'arrestation et de notices rouges étrangères.*

Afin de veiller au nécessaire ***caractère transversal*** *des trois canaux de coopération, un point de contact central a été désigné à la SCCOPOL en août 2004. La principale fonction de celui-ci est d'aider les services répressifs français à choisir le meilleur outil de coopération policière en fonction de la nature et de la complexité des enquêtes en cours. Il contrôle la légalité de la demande, procède aux premiers contrôles croisés et transmet ladite demande vers le canal de coopération le plus approprié en tenant compte de la demande des enquêteurs. Seules les demandes relatives à un signalement Schengen relèvent de la compétence exclusive du bureau SIRENE France.*

Par suite d'une mise en commun réussie des ressources, la SCCOPOL traite, ***24 heures sur 24****, près de* ***350 000 messages par an****, sur une* ***plateforme sécurisée unique****, avec des effectifs limités.*

La compétence multicanale de la SCCOPOL lui permet de représenter la France au sein des groupes européens (SIS/VIS, SIS/SIRENE, chefs d'UNE) ou d'Interpol (réunion des agents de contact d'Interpol, groupe "Notices") et d'apporter un point de vue opérationnel pertinent à l'unité DRI qui est chargée en France du suivi des organes de gouvernance d'Interpol et d'Europol.

1.2. Bureaux SIRENE

Les bureaux SIRENE sont essentiels pour le fonctionnement du SIS et l'échange d'informations. Dans chaque État membre, des bureaux SIRENE (supplément d'information requis à l'entrée nationale) permanents sont mis en place dans le cadre de l'acquis de Schengen[8] pour jouer le rôle d'instance désignée ayant la compétence centrale pour la partie nationale du système d'information Schengen (SIS II). Ils servent de point de contact pour les bureaux SIRENE des autres parties contractantes, ainsi que pour la liaison avec les autorités et agences nationales. Le SIS II est un système de concordance/non-concordance ("hit/no hit") fondé sur des recherches. Sur la base d'un fonctionnement assuré 24 heures sur 24 et 7 jours sur 7, les bureaux échangent des données relatives aux signalements du SIS II[9], un signalement étant un ensemble de données permettant aux autorités d'identifier des personnes ou des objets en vue de prendre des mesures appropriées.

On entend par "informations supplémentaires", les informations non stockées dans le SIS II, mais en rapport avec des signalements introduits dans le SIS II, qui doivent être échangées, de manière bilatérale ou multilatérale, au moyen de formulaires:

i) afin de permettre aux États membres de se consulter ou de s'informer mutuellement lors de l'introduction d'un signalement;

ii) à la suite d'une réponse positive afin que la conduite à tenir appropriée puisse être exécutée;

iii) en cas d'impossibilité d'exécuter la conduite à tenir demandée;

iv) en ce qui concerne la qualité des données du SIS II;

v) en ce qui concerne la compatibilité et la priorité des signalements;

vi) en ce qui concerne l'exercice du droit d'accès.

---

[8] Voir la Convention d'application de l'Accord de Schengen, JO L 239 du 22.9.2000, p. 19.

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

Les informations doivent être échangées conformément aux dispositions du manuel SIRENE[10] et au moyen de l'infrastructure de communication[11]. Le SIS II[12] est doté de fonctionnalités renforcées par rapport à son prédécesseur, permettant par exemple d'enregistrer des empreintes digitales, des photographies et de nouveaux types d'objets (aéronefs, embarcations, conteneurs et moyens de paiement volés), ainsi que, pour le propriétaire du signalement, d'établir un lien entre différents signalements. Dans le SIS II, une copie des mandats d'arrêts européens (MAE) est directement jointe aux signalements relatifs aux personnes concernées.

Les bureaux SIRENE facilitent la coopération en matière policière et peuvent également jouer un rôle dans l'échange d'informations ne relevant pas du champ d'application du SIS II au titre des dispositions, précédemment couvertes par les articles 39 et 46 de la CAAS, qui ont été remplacées par **la "décision-cadre suédoise"**. Conformément à l'article 12, paragraphe 1, de la "décision-cadre suédoise", les dispositions de l'article 39, paragraphes 1, 2 et 3, et de l'article 46 de la Convention d'application de l'Accord de Schengen (CAAS), dans la mesure où elles ont trait à l'échange d'informations ou de renseignements afin de mener des enquêtes pénales ou des opérations de renseignement en matière pénale dans les conditions prévues par la présente décision-cadre, sont remplacées par les dispositions de la présente décision-cadre.

1.3. Unité nationale Europol (UNE)

Chaque État membre a son unité nationale Europol (UNE) désignée, qui sert d'organe de liaison entre Europol et les autorités nationales compétentes. Les officiers de liaison (OL) détachés par les UNE auprès d'Europol devraient assurer une liaison permanente, 24 heures sur 24 et 7 jours sur 7, entre le siège d'Europol à La Haye et les unités nationales Europol installées dans les 28 États membres. Europol accueille également des OL de 10 pays tiers et organisations. Le réseau peut compter sur des canaux de communication sécurisés fournis par Europol.

---

10 Décision d'exécution de la Commission du 26 février 2013 relative au manuel Sirene et à d'autres mesures d'application pour le système d'information Schengen de deuxième génération (SIS II) [notifiée sous le numéro C(2013) 1043], JO L 71 du 14.3.2013, p. 1.

11 En raison de la fermeture du réseau SISNET Mail, les bureaux SIRENE peuvent désormais utiliser le service de courrier s-TESTA. D'autres échanges d'informations peuvent avoir lieu via les canaux de communication du réseau s-TESTA, de SIENA ou de I-24/7.

12 Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation du système d'information Schengen de deuxième génération (SIS II), conformément à l'article 24, paragraphe 5, à l'article 43, paragraphe 3, et à l'article 50, paragraphe 5, du règlement (CE) n° 1987/2006, ainsi qu'à l'article 59, paragraphe 3, et à l'article 66, paragraphe 5, de la décision 2007/533/JAI; doc. 15810/16 SIRIS 175 COMIX 860.

Europol[13] soutient les services répressifs des États membres en matière de prévention de la criminalité organisée, de la grande criminalité internationale et du terrorisme qui affectent deux États membres ou plus, ainsi que de lutte contre ces phénomènes. Afin de recueillir, de stocker, de traiter et d'analyser les données à caractère personnel et d'échanger des informations et des renseignements, Europol est tributaire de la fourniture de données par les États membres. Le règlement Europol fixe les différentes tâches en matière d'informations, ainsi que les règles relatives à l'utilisation de données et à leur échange avec des tiers sur la base d'un régime solide dans le domaine de la protection et de la sécurité des données.

1.4. Bureaux centraux nationaux d'INTERPOL (BCN)

Les **bureaux centraux nationaux (BCN)** présents aux sièges des polices nationales jouent un rôle central pour le traitement, dans le cadre du système d'information d'Interpol, des données fournies par leur pays. Ils ont le droit d'accéder directement au système, notamment en ce qui concerne:

- l'enregistrement, la mise à jour et la suppression des données directement dans les bases de données policières de l'organisation, ainsi que la création de liens entre les données;
- la consultation directe de ces bases de données;
- l'utilisation des notices et des circulaires d'Interpol pour la transmission des demandes de coopération et des signalements internationaux.

Les BCN peuvent consulter et recouper rapidement les données par un accès direct, assuré 24 heures sur 24 et 7 jours sur 7, à des bases de données contenant des informations sur des terroristes présumés, des personnes recherchées, des empreintes digitales, des profils ADN, des documents de voyage perdus ou volés, des véhicules à moteur volés, des œuvres d'art volées etc.

---

[13] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à partir du 1er mai 2017).

Dans la mesure du possible, les BCN devraient permettre aux autorités qui sont chargés des poursuites pénales dans leur pays et participent à la coopération policière internationale d'avoir accès au système d'information d'Interpol. Les BCN contrôlent le niveau d'accès que d'autres utilisateurs autorisés de leurs pays ont aux services d'Interpol et peuvent demander à être informés des requêtes effectuées dans leurs bases de données nationales par d'autres pays.

1.5. Points de contact nationaux Prüm

Les "décisions Prüm"[14] ont conféré une nouvelle dimension transfrontière à la lutte contre la criminalité en fournissant un accès mutuel transfrontière en ligne aux bases de données de profils ADN nationales désignées, au système de reconnaissance automatisée d'empreintes digitales (AFIS) et aux bases de données relatives à l'immatriculation des véhicules (DIV). Afin de fournir des données, un point de contact national (PCN) est désigné pour chaque type d'échange de données dans chaque État membre participant[15]. La protection des données et les dispositions ciblées en matière de sécurité des données tiennent particulièrement compte de la nature spécifique de l'accès en ligne à ces bases de données. La fourniture de données à caractère personnel suppose un niveau de protection des données et de sécurité qui soit suffisant, testé en commun et convenu par les États membres avant le démarrage de l'échange de données.

1.5.1. PCN Prüm - ADN et empreintes digitales

Dans le cas des profils ADN et des données dactyloscopiques, la comparaison automatisée de données repose sur un système "hit - no hit". Les données de référence ne permettent l'identification immédiate de la personne concernée. En cas de résultat positif ("hit"), le PCN de l'État membre qui effectue la consultation peut donc demander des données à caractère personnel supplémentaires bien précises. La fourniture de telles données supplémentaires doit être demandée par le biais de procédures d'entraide judiciaire, notamment celles adoptées conformément à la "décision-cadre suédoise", et elle relève du droit national de l'État membre requis, y compris les dispositions relatives à l'entraide judiciaire.

---

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

15 Doc. 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Guide des bonnes pratiques relatif aux recherches d'empreintes digitales

Lors de l'utilisation de la fonction de recherche automatisée d'empreintes digitales dans le cadre de Prüm, l'État membre requérant devrait suivre les recommandations figurant dans le document *Bonnes pratiques en matière d'interrogation des bases de données des États membres* (doc. 14885/1/08 REV 1). On y prend acte des capacités de recherche limitées dans les **bases de données dactyloscopiques** et on y recommande de promouvoir les pratiques ci-après au niveau opérationnel:

- La consultation ou non des bases de données d'empreintes digitales des États membres et l'ordre dans lequel les recherches y sont effectuées relèvent de décisions qui sont prises pour chaque enquête au cas par cas et ne devraient pas être fixées à l'avance de manière systématique.

- Les bases de données d'empreintes digitales des autres États membres ne devraient en principe pas être utilisées tant que la ou les propres bases de données d'empreintes digitales de l'État membre requérant n'ont pas été exploitées.

- Pour décider d'effectuer ou non une recherche dans les bases de données d'un ou de plusieurs États membres, il convient en particulier de tenir compte:

  – de la gravité de l'affaire;

  – et/ou de pistes à creuser dans le cadre de l'enquête, notamment d'informations qui mènent vers un État membre ou un groupe d'États membres;

  – et/ou des exigences spécifiques de l'enquête.

- Des recherches générales ne devraient être menées que lorsque les bonnes pratiques visées aux points 1 à 3 n'ont pas données de résultats.

Exemples d'échange de données automatisé au titre des décisions Prüm du Conseil

En 2011, du matériel génétique a été enregistré dans la base de données ADN nationale tchèque lors d'une enquête concernant un meurtre. L'enquête a été dirigée contre un suspect qui avait fui à l'étranger. Le matériel génétique provenait d'un mégot de cigarette retrouvé dans un cendrier à l'intérieur de l'appartement dans lequel le crime avait été commis. Une recherche effectuée dans la base de données ADN autrichienne en 2014 a révélé que le même profil avait été traité en Autriche. D'autres données à caractère personnel ont été échangées par les PCU des deux pays dans le cadre de la coopération policière. Ensuite, le service autrichien de justice pénale a été contacté et il lui a été demandé de remettre le suspect à la République tchèque aux fins de poursuites pénales, par le biais de l'entraide judiciaire en matière pénale.

En 2005, un profil ADN a été enregistré dans la base de données ADN nationale tchèque lors d'une enquête concernant un vol. Un suspect a été identifié en 2014 après la consultation de la base de données ADN autrichienne. La partie autrichienne a été invitée à fournir une photographie récente et d'autres données à caractère personnel par l'intermédiaire des PCU.

1.5.2. PCN Prüm - Données d'immatriculation des véhicules (DIV)

En ce qui concerne les DIV, les recherches peuvent être menées à partir d'un numéro de châssis complet dans un ou tous les États membres participants, ou d'un numéro d'immatriculation complet dans un État membre particulier. Les informations seront échangées par les PCN désignés tant pour les demandes entrantes que pour les demandes sortantes. Les États membres s'accordent mutuellement un accès en ligne aux données nationales d'immatriculation des véhicules (DIV) pour:

a) les données relatives aux propriétaires ou aux détenteurs, et

b) les données relatives aux véhicules.

Les États membres utilisent une version de l'application logicielle du système d'information européen concernant les véhicules et les permis de conduire (EUCARIS) qui est spécialement conçue pour mener à bien ces recherches aux fins de Prüm. Les recherches portant sur les DIV diffèrent des celles concernant l'ADN et les empreintes digitales dans la mesure où elles renvoient à la fois des données à caractère personnel et des données de référence en cas de résultat positif ("hit"). Tout comme pour d'autres consultations automatisées, il est entendu que la transmission de données à caractère personnel est soumise à l'application d'un niveau de protection des données approprié par l'État membre destinataire.

1.5.3. PCN Prüm en matière de prévention du terrorisme

Sur demande ou de leur propre initiative, les PCN désignés peuvent échanger des informations concernant des personnes soupçonnées de commettre des infractions terroristes. Les données comporteront le nom, les prénoms, la date et le lieu de naissance du suspect, ainsi qu'une description des circonstances qui sont à l'origine de la présomption selon laquelle la personne concernée s'apprête à commettre des infractions pénales en rapport avec des activités terroristes.

L'État membre qui transmet les données peut, conformément au droit national, fixer des conditions d'utilisation de ces données et informations par l'État membre qui les reçoit, ce dernier étant tenu de respecter lesdites conditions.

1.5.4. PCN Prüm en matière d'événements majeurs

Les États membres qui accueillent des événements majeurs de dimension internationale doivent assurer la sécurité tant du point de vue de l'ordre public que de la lutte contre le terrorisme. En fonction de la nature de l'événement (politique, sportive, sociale, culturelle ou autre), l'un de ces aspects peut être plus important que l'autre. Toutefois, les deux aspects doivent être pris en considération bien qu'ils puissent éventuellement être traités par des autorités différentes. Une attention particulière est accordée au phénomène des déplacements de délinquants violents, notamment en ce qui concerne les matchs de football de dimension internationale.

Aux fins de la prévention des infractions pénales et du maintien de l'ordre public et de la sécurité en liaison avec des événements majeurs et des manifestations de masse similaires (d'ordre politique, sportif, social, culturel ou autre), des catastrophes et des accidents graves ayant des implications transfrontières, les PCN désignés se transmettent les uns aux autres, sur demande ou de leur propre initiative:

- des données à caractère non personnel, ou
- des données à caractère personnel, lorsque des condamnations définitives ou d'autres circonstances font présumer que les personnes concernées vont commettre des infractions pénales dans le cadre de ces événements ou qu'elles présentent un danger pour l'ordre public et la sécurité.

Les données à caractère personnel ne peuvent être traitées qu'aux fins susmentionnées et pour les manifestations précises en vue desquelles elles ont été communiquées. Les données transmises doivent être effacées immédiatement, dès lors que ces objectifs ont été atteints et, dans tous les, cas après un an au plus. Les informations sont fournies dans le respect du droit national de l'État membre qui les transmet.

1.5.4.1. Manuel de coopération lors d'événements majeurs revêtant une dimension internationale[16]

Ce manuel contient des orientations et des suggestions destinées aux services répressifs chargés d'assurer la sécurité publique lors d'évènements majeurs tels que les Jeux olympiques et d'autres grandes manifestations sportives, des événements à caractère social ou des réunions politiques de haut niveau.

Le manuel, qui est constamment modifié et adapté en fonction de l'évolution des meilleures pratiques, comporte des recommandations sur la gestion de l'information et des événements, ainsi que sur l'évaluation stratégique et liée à l'évènement. Les formulaires types fournis en annexe concernent:

- les demandes d'envoi d'officiers de liaison;
- l'analyse des risques afférents aux manifestants potentiels et autres groupes;
- l'échange d'informations concernant des individus ou des groupes représentant une menace terroriste;
- une liste de documents de référence;
- un tableau de points de contact nationaux permanents dans le domaine de l'ordre public.

1.6. Points nationaux (policiers) d'information "football" (PNIF)[17]

En plus des PCN Prüm en matière d'événements majeurs et notamment en ce qui concerne les matchs de football de dimension internationale, un point national d'information "football" (PNIF) présent dans chaque État membre est chargé de l'échange d'informations pertinentes et du développement de la coopération policière transfrontière. Des informations tactiques, stratégiques et opérationnelles peuvent être utilisées par le PNIF lui-même ou être transmises aux autorités ou aux services de police intéressés.

Les contacts entre les services de police des différents pays concernés par un événement sont coordonnés et, si nécessaire, organisés par le PNIF. Le site web de la Centrale d'information sur le hooliganisme dans le football (CIV) destiné aux PNIF (www.nfip.eu) diffuse des informations et des avis sur les possibilités juridiques et autres qui sont disponibles dans le domaine de la sûreté et de la sécurité lors des matchs de football.

---

[16] Recommandation 2007/C 314/02 du Conseil du 6 décembre 2007 relative à un Manuel destiné aux autorités de police et de sécurité concernant la coopération lors d'événements majeurs revêtant une dimension internationale, JO C 314 du 22.12.2007, p. 4.

[17] Décision 2002/348/JAI du Conseil du 25 avril 2002 concernant la sécurité lors de matches de football revêtant une dimension internationale, JO L 121 du 8.5.2002, p. 1.

Le PNIF coordonne le traitement des informations relatives aux supporteurs à risques, à des fins de préparation et de prise des mesures appropriées pour assurer le maintien de l'ordre à l'occasion d'une rencontre de football. De telles informations incluent, notamment, des données relatives à des individus qui présentent ou peuvent présenter un danger pour l'ordre public et la sécurité. Il convient d'échanger les informations concernées au moyen des formulaires[18] figurant dans l'appendice du manuel concernant les matchs de football.

1.6.1. Manuel concernant les matchs de football[19]

Le manuel concernant les matchs de football figure en annexe de la résolution 2016/C 444/01 et fournit des exemples de la manière dont la police devrait coopérer au niveau international afin de prévenir et de maîtriser la violence et les troubles liés aux matchs de football. Son contenu consiste notamment en des recommandations concernant:

- la gestion des informations par les services de police;
- l'organisation de la coopération entre les forces de police;
- une liste des points à vérifier (destinée à la police et aux pouvoirs publics) en ce qui concerne la politique médiatique et la stratégie de communication.

---

18 Décision 2007/412/JAI du Conseil du 12 juin 2007 modifiant la décision 2002/348/JAI concernant la sécurité lors de matches de football revêtant une dimension internationale, JO L 155 du 15.6.2007, p. 76.

19 Résolution du Conseil concernant un manuel actualisé assorti de recommandations pour la mise en place, à l'échelle internationale, d'une coopération policière et de mesures visant à prévenir et à maîtriser la violence et les troubles liés aux matchs de football revêtant une dimension internationale qui concernent au moins un État membre ("manuel de l'Union européenne concernant les matchs de football"), JO C 444 du 29.11.2016, p. 1.

1.7. Points focaux nationaux sur les armes à feu

Dans le prolongement du plan d'action de l'UE du 2 décembre 2015 (COM(2015) 624 final), sous la rubrique intitulée "Améliorer la connaissance de la situation grâce au renseignement", la Commission a invité tous les États membres à créer des points focaux nationaux interconnectés sur les armes à feu et à mettre en réseau ces points focaux afin de développer leur expertise et d'améliorer l'analyse et l'établissement de rapports stratégiques sur le trafic d'armes à feu, notamment par l'exploitation combinée de renseignements de nature pénale et balistique.

La stratégie de l'UE contre les armes à feu et armes légères et de petit calibre illicites et leurs munitions, intitulée "Sécuriser les armes, protéger les citoyens"[20], indique, sous la rubrique "Respect des règles par des mesures de suivi et de contrôle de leur application - coopération opérationnelle", que "l'UE améliorera la coopération transfrontière entre autorités judiciaires et répressives, encouragera les autorités compétentes des États membres, y compris les autorités douanières, à établir des points focaux nationaux sur les armes à feu, améliorera l'analyse de l'ensemble des informations disponibles en matière d'armes à feu illicites et veillera à une totale participation à l'échange d'informations avec Europol en ce qui concerne le trafic d'armes à feu." Ce document a été approuvé par le Conseil, qui en a fait une stratégie de l'UE à part entière[21].

Les points focaux nationaux sur les armes à feu ont pour objectif de collecter et d'analyser les informations ainsi que d'améliorer les flux d'informations concernant l'utilisation d'armes à feu à des fins criminelles et le trafic d'armes à feu à destination et à l'intérieur des États membres et dans toute l'UE, tant au niveau stratégique qu'au niveau opérationnel, au moyen d'une collecte et d'un partage coordonnés d'informations afin d'améliorer la connaissance de la situation grâce au renseignement et de mieux informer les services répressifs Les informations devraient être échangées selon les lignes directrices contenues dans le guide EFE & EMPACT sur les bonnes pratiques en matière d'armes à feu.

---

20 JOIN(2018) 17 final du 1.6.2018.

21 Conclusions du Conseil du 19 novembre 2018 – Document 13581/18.

1.7.1. Guide sur les bonnes pratiques concernant les points focaux nationaux sur les armes à feu

Le guide sur les bonnes pratiques[22] en vue de la mise en place de points focaux nationaux sur les armes à feu fournit des exemples sur la manière dont les points focaux nationaux devraient accomplir les tâches suivantes:

- création d'un registre de renseignements relatifs aux armes à feu, de nature pénale et balistique,
- création d'un registre répertoriant toutes les armes à feu perdues, volées et récupérées,
- traçage de toutes les armes à feu saisies, depuis le fabricant jusqu'au dernier propriétaire légal,
- analyse des données de traçage des armes à feu afin d'identifier le type, la marque, le modèle, le calibre et le pays de fabrication,
- fourniture de données, de statistiques, d'informations, d'évaluations et de rapports à l'usage des États membres,
- servir de point de contact technique avec l'ONUDC,
- assurer le respect des exigences liées au questionnaire des Nations unies sur les flux illicites d'armes,
- favoriser la coopération internationale.

En ayant accès aux bases de données pertinentes, y compris le système d'information Europol (SIE), le système d'information Schengen (SIS II) et le système iARMS, et en suivant le guide sur les bonnes pratiques, les points focaux nationaux sur les armes à feu devraient être en mesure d'entreprendre et d'assurer l'échange d'informations, de lancer des demandes de recherche internes et entrantes, d'assister et de coordonner les actions opérationnelles tout en maintenant un contrôle suffisant des renseignements, des données et des informations au niveau national, permettant ainsi une diffusion rapide et régulière de ces données à Europol et à d'autres institutions et agences répressives telles que l'ONUDC.

[22] 8586/18.

1.8. Centres de coopération policière et douanière (CCPD)

Les CCPD sont institués sur la base d'accords multilatéraux conclus conformément à l'article 39, paragraphe 4, de la Convention d'application de l'accord de Schengen (CAAS). Par ces accords, les États parties contractantes définissent, dans les grandes lignes, les bases de leur coopération transfrontière, notamment les missions, le cadre juridique et les règles de création et de fonctionnement des centres. Les CCPD regroupent des agents de pays voisins et sont étroitement liés aux organismes nationaux de coopération internationale (PCN, BCN Interpol, UNE, bureaux SIRENE).

Les CCPD donne des conseils et apporte un soutien non opérationnel aux forces de police, aux douanes et à d'autres services opérationnels nationaux dans la région frontalière où ils sont situés. Les agents des CCPD ont pour mission de fournir rapidement les informations demandées, conformément à la décision 2006/960/JHA du Conseil ("décision-cadre suédoise").

À la fin de l'année 2016, 8 des 59 CCPD existants étaient reliés à SIENA, l'application de réseau d'échange sécurisé d'informations d'Europol. L'échange d'informations par le biais du CCPD concerne en particulier la petite et moyenne délinquance, les flux migratoires illégaux et les problèmes d'ordre public. Il peut s'agir notamment de l'identification de conducteurs de véhicules ou de la vérification de la pertinence et de l'authenticité de documents d'identité ou de voyage.

Sur décision conjointe des parties contractantes, le CCPD peut être érigé en centre opérationnel régional de coordination à la disposition de l'ensemble des services concernés, notamment en cas d'événements régionaux fortuits (catastrophe naturelle) ou de grands événements (G8, Jeux olympiques, coupe du monde de football, etc.).

Si un CCPD est destinataire d'une information relevant de la compétence des organes centraux nationaux, il devra la répercuter au PCU/à l'organe central sans délai. Dans le cas où un CCPD reçoit des informations dont l'intérêt est évident pour Europol, il peut les transmettre à l'UNE située au sein du PCU qui les adressera à Europol.

Exemple d'échange d'informations par l'intermédiaire d'un CCPD

L'EPICC ("Euregio Police Information and Cooperation Centre" ou centre eurégional pour la coopération et l'information en matière de police) est le nom abrégé du CCPD Heerlen.

Il a été créé de manière ad hoc (sans instrument juridique particulier) en 2005, à l'initiative de "NeBeDeAgPol"", une association des responsables de la police dans l'Euregio Meuse-Rhin, située dans la région frontalière entre les Pays-Bas, la Belgique et l'Allemagne - l'une des zones frontalières les plus densément peuplées dans l'Union européenne.

Au sein de ce CCPD, environ trente fonctionnaires de police belges, allemands et néerlandais travaillent ensemble sur une même plateforme.

Ils ont accès sur place à la plus grande partie du contenu des bases de données de leurs pays respectifs. Cela leur permet d'apporter - dans un très court délai - des réponses exactes, complètes et fiables aux demandes d'informations de la police concernant la Belgique, l'Allemagne et les Pays-Bas. L'échange d'informations entre les trois délégations de l'EPICC s'effectue par l'intermédiaire de l'application "SIENA" d'Europol.

L'EPICC recueille et analyse les informations policières disponibles dans la région frontalière afin de détecter, de décrire et de suivre les problèmes relatifs à la sécurité des frontières (nouveaux phénomènes ou modes opératoires, groupes de criminels agissant dans la région frontalière, événements ou personnes nécessitant une attention particulière, etc.).

Grâce à son expertise spéciale et sa composition mixte, le CCPD Heerlen peut apporter une aide efficace lors de la préparation et de la mise en œuvre d'opérations, d'enquêtes ou de mesures de surveillance transfrontières.

1.9. Officiers de liaison

D'après l'article 47 de la convention d'application de l'accord de Schengen (CAAS), les États membres *"peuvent conclure des accords bilatéraux permettant le détachement, pour une durée déterminée ou indéterminée, de fonctionnaires de liaison (...) [d'un État membre] auprès de services de police de l'autre (...) [État membre]"*. Le rôle des officiers de liaison est d'établir et de maintenir des contacts directs afin d'approfondir et d'accélérer la coopération en vue de la lutte contre la criminalité, notamment en fournissant une assistance. Les officiers de liaison ne sont pas habilités à appliquer des mesures de police de manière autonome. Ils garantissent une coopération rapide et efficace, fondée sur des contacts personnels et de la confiance mutuelle:

- en facilitant et en accélérant la collecte et l'échange d'informations;
- en exécutant des demandes d'entraide policière et judiciaire en matière pénale;
- en organisant et en assurant des opérations transfrontières.

Les officiers de liaison peuvent être affectés dans d'autres États membres, dans des pays tiers, ainsi que dans des agences de l'UE ou des organisations internationales. Le répertoire[23] des fonctionnaires de liaison des services répressifs, mis à jour chaque année par le Secrétariat général du Conseil, explique le travail et les tâches des officiers de liaison et contient une liste d'officiers de liaison ainsi que de leurs coordonnées.

À la lumière des expériences passées et en cours dans différents pays d'accueil, ainsi qu'en vue de parvenir à une plus grande mutualisation des activités des États membres vis-à-vis des pays tiers, tant en ce qui concerne le travail des officiers de liaison que la coopération technique, un certain nombre de bonnes pratiques ont été identifiées et figurent dans le répertoire. Il est suggéré que les officiers de liaison des États membres et leurs autorités compétentes appliquent lesdites bonnes pratiques lorsque cela est approprié.

---

[23] Mise à jour (2018) du répertoire des agents de liaison des services répressifs ("Compendium on law enforcement liaison officers"), doc. 10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422.

Exemples typiques d'échange d'informations entre officiers de liaison

- *Les officiers de liaison peuvent être chargés d'assurer les contacts afin d'établir une coopération directe dans des cas spécifiques tels que de la criminalité liée à la drogue.*
- *Les officiers de liaison peuvent fournir des informations spécifiques sur la règlementation et la législation nationales en ce qui concerne la coopération policière internationale ou l'entraide judiciaire en matière pénale.*
- *Les officiers de liaison maintiennent, dans certains cas, des listes actualisées des autorités responsables au sein de leur État membre.*
- *Les officiers de liaison ont également été invités, dans certains États membres, à traiter les demandes de coopération au titre de l'article 17 de la décision de Prüm (opérations conjointes). Ainsi, par exemple, l'officier de liaison danois au sein d'Europol a été invité par la République tchèque à transmettre une demande au Danemark en vue de l'affectation de quatre fonctionnaires de police danois pour l'assister dans une affaire concernant les deux États membres.*

1.10. Bureaux de recouvrement des avoirs (BRA) des États membres

La criminalité financière couvre un large éventail d'activités telles que la contrefaçon, la corruption et la fraude (comme, par exemple, l'escroquerie à la carte de crédit, le stellionat, la fraude médicale ou la contrefaçon de titres, la corruption ou le détournement de fonds, le blanchiment d'argent, l'usurpation d'identité et l'évasion fiscale). Une meilleure coopération peut être obtenue par une collaboration transfrontière plus étroite entre les bureaux de recouvrement des avoirs (BRA), les cellules de renseignement financier (CRF) et les autorités policières et douanières[24].

[24] Manuel des bonnes pratiques en matière de lutte contre la criminalité financière: une série de bons exemples de systèmes élaborés, mis sur pied dans les États membres pour lutter contre la criminalité financière, doc. 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

À la suite de l'adoption de la décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime[25], tous les États membres ont depuis établi et désigné des bureaux de recouvrement des avoirs (BRA). Ces unités spécialisées ont évolué pour devenir un réseau étroitement intégré de spécialistes qui peuvent s'échanger directement des informations sur les questions relatives au recouvrement des avoirs en ayant recours au système SIENA. Sous l'égide de la Commission européenne et d'Europol, le réseau des BRA facilite la coopération entre les bureaux de recouvrement des avoirs des États membres, ainsi que la discussion stratégique et l'échange de bonnes pratiques. Le Bureau des avoirs d'origine criminelle d'Europol (ECAB, "Europol Criminal Assets Bureau") joue un rôle de coordination dans le cadre du recouvrement des avoirs au sein de l'UE.

Les dispositions fixées par la directive 2014/42/UE du Parlement européen et du Conseil du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne[26] permettront de poursuivre le renforcement de l'efficacité de la coopération entre les bureaux de recouvrement des avoirs au sein de l'Union européenne. Les États membres sont invités à transposer la directive au plus tard le 4 octobre 2016.

Le **Réseau Camden regroupant les autorités compétentes en matière de recouvrement d'avoirs (CARIN)**, mis en place en 2004 en appui à l'identification, au gel, à la saisie et à la confiscation transfrontières de biens en rapport avec le crime, renforce l'échange mutuel d'informations en ce qui concerne différentes approches nationales dont la portée s'étend au-delà de l'UE.

Depuis 2015, le réseau CARIN comprend des praticiens de 53 juridictions et de 9 organisations internationales, qui servent de points de contact aux fins d'échange transfrontière rapide d'informations, sur demande ou de manière spontanée. Les BRA nationaux coopèrent entre eux ou avec d'autres autorités qui facilitent le dépistage et l'identification des produits du crime. Si tous les États membres ont mis en place leur BRA, il existe néanmoins de grandes différences entre les États membres en termes d'organisation, de ressources et d'activités.

---

[25] Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime, JO L 332 du 18.12.2007, p. 103.

[26] Directive 2014/42/UE du Parlement européen et du Conseil du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne, JO L 127 du 29.4.2014, p. 39.

Les informations échangées peuvent être utilisées conformément aux dispositions en matière de protection des données de l'État membre destinataire et sont soumises aux mêmes règles de protection des données que si elles avaient été recueillies dans l'État membre destinataire. L'échange spontané d'informations effectué conformément à cette décision, en appliquant les procédures et délais prévus par la décision-cadre suédoise, doit être encouragé.

1.11. Blanchiment de capitaux - Coopération entre cellules de renseignement financier CRF)[27] [28]

Des informations pertinentes sur tout fait qui pourrait être l'indice d'un blanchiment de capitaux ou d'un financement du terrorisme devraient être communiquées aux cellules nationales de renseignement financier (CRF). Les CRF analysent les informations reçues au cas par cas de façon à faire le lien entre les transactions suspectes et les activités criminelles sous-jacentes en vue de prévenir et de combattre le blanchiment de capitaux et le financement du terrorisme. Les CRF font office de cellules nationales centrales pour la réception, l'analyse et la dissémination des résultats de leurs analyses aux autorités compétentes. Étant fonctionnellement indépendantes et autonomes, les CRF exercent leurs fonctions librement, y compris pour décider d'une manière autonome d'analyser, de demander et de disséminer des informations particulières.

Les CRF servent également de points de contact nationaux pour l'échange transfrontière d'informations. À l'instar des autorités compétentes en matière de recouvrement d'avoirs, elles diffèrent considérablement selon les États membres en termes d'organisation, de fonctions et de ressources. Elles sont placées sous la dépendance des autorités judiciaires ou de services de police ou créées comme des organes "hybrides", combinant compétences de police et du parquet. Une telle diversité peut parfois susciter des obstacles dans la coopération internationale.

---

[27] Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil, JO L 186 du 11.7.2019, p. 122.

[28] Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, JO L 141 du 5.6.2015, p. 73.

Toutefois, compte tenu du caractère transnational du blanchiment de capitaux et du financement du terrorisme, la coordination et la coopération entre les CRF sont extrêmement importantes. Afin d'améliorer cette coordination et cette coopération et de garantir que les déclarations de transactions suspectes parviennent bien à la CRF de l'État membre où elles seraient le plus utiles, la directive (UE) 2015/849 contient des règles détaillées. En vue de mettre en œuvre rapidement, dans un esprit constructif et de manière effective la coopération transfrontière la plus étendue possible, les États membres devraient en particulier veiller à ce que leurs CRF échangent des informations, librement, spontanément ou sur demande, avec les cellules de renseignement financier de pays tiers.

Il convient d'améliorer l'échange d'informations entre CRF au sein de l'Union et l'utilisation de systèmes sécurisés, en particulier le réseau informatique décentralisé CRF.NET. Les 28 CRF sont toutes connectées à CRF.NET. Ce réseau a été développé au cours des dernières années, transformant un outil de base sécurisé pour l'échange bilatéral structuré d'informations en un outil multifonctionnel sécurisé pour l'échange multilatéral d'informations prévoyant des fonctionnalités de gestion des dossiers ainsi qu'une normalisation semi-automatisée des processus. Dans CRF.NET, chaque nouvelle fonctionnalité et chaque nouveau processus automatisé sont facultatifs et ne sont assortis d'aucune restriction. Les différentes CRF peuvent décider quels sont les possibilités et fonctionnalités de CRF.NET qu'elles utilisent; elles n'ont recours qu'aux fonctionnalités qui leur conviennent et excluent celles dont elles n'ont pas besoin ou auxquelles elles n'ont pas envie de faire appel.

1.12. Convention Naples II[29]

Les États membres se prêtent assistance mutuelle dans le cadre de la convention Naples II en vue de prévenir et de détecter les infractions aux réglementations douanières nationales, ainsi que de poursuivre et de réprimer les infractions aux réglementations douanières communautaires et nationales. En ce qui concerne les enquêtes pénales, la convention établit les procédures dans le cadre desquelles les administrations douanières peuvent agir conjointement et s'échanger des données, spontanément ou sur demande, en matière de trafics illicites.

Les demandes sont soumises par écrit dans une langue officielle de l'État membre de l'autorité requise ou dans une langue acceptable pour cette autorité. Un formulaire fixe la norme en matière de communication d'informations. Les autorités concernées communiquent toutes les informations susceptibles d'aider à prévenir, à détecter et à poursuivre les infractions. Elles échangent des données à caractère personnel, c'est-à-dire toutes les informations qui se rapportent à une personne physique identifiée ou identifiable.

---

[29] Acte du Conseil du 18 décembre 1997 établissant, sur la base de l'article K.3 du traité sur l'Union européenne, la convention relative à l'assistance mutuelle et à la coopération entre les administrations douanières, JO C 24 du 23.1.1998, p. 4.

Dans le cadre de l'assistance prêtée, l'autorité requise, ou l'autorité compétente saisie par cette dernière, procède comme si elle agissait pour son propre compte ou à la demande d'une autre autorité de son propre État membre.

Le mémento pour la convention de Naples II relative à l'assistance mutuelle et à la coopération entre les administrations douanières est subdivisé en trois parties:

- les dispositions générales figurent dans le document 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- les fiches nationales, mises à jour en 2016, figurent dans le document 15429/16 JAI 1028 ENFOCUSTOM 238;
- les annexes, y compris les formulaires types de transmission d'informations, figurent dans le document 13615/05 ENFOCUSTOM 61 ADD 1.

1.13. Unité d'informations passagers (UIP)

Dans le cadre de la directive 2016/681[30], chaque État membre met en place ou désigne une unité d'informations passagers (UIP). Ces unités sont compétentes pour traiter les données des dossiers passagers (PNR) qu'elles reçoivent des transporteurs aériens[31] et constituent en outre le principal canal d'échange d'informations entre les États membres et avec Europol. Deux États membres ou plus peuvent mettre en place ou désigner une autorité unique en tant qu'UIP commune.

Le traitement des données PNR sert principalement à évaluer les passagers aériens afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités nationales compétentes en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière. La directive s'applique aux vols extra-UE mais peut également concerner les vols intra-UE si un État membre le décide.

---

30 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO L 119 du 4.5.2016, p. 132.

31 La directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

L'évaluation des données PNR facilite l'identification de personnes qui, avant cette évaluation, n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité. Conformément à la politique menée par l'UE en matière de protection des données, le traitement de ce type de données devrait être à la fois pertinent et nécessaire, tout en étant proportionné aux objectifs de sécurité spécifiques poursuivis par la directive.

Les UIP sont chargées:

- au niveau national, de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités nationales compétentes;

- au niveau de l'Union, de l'échange des données PNR et du résultat du traitement de celles-ci

    a) entre elles. Dans les cas d'urgence, cependant, et sous certaines conditions, les autorités nationales compétentes susmentionnées peuvent demander directement à l'UIP d'un autre État membre de leur communiquer des données PNR qui sont conservées dans sa base de données; et

    b) avec Europol, qui est habilitée, dans les limites de ses compétences et pour l'accomplissement de ses missions, à demander de telles données aux UIP.

Les UIP s'acquittent exclusivement de leurs tâches dans un endroit sécurisé situé sur le territoire d'un État membre. Les données PNR communiquées aux UIP doivent être stockées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre d'arrivée ou de départ. Toutefois, six mois après leur transfert, toutes les données PNR doivent être dépersonnalisées par le masquage des éléments des données qui sont indiqués dans la directive et pourraient servir à identifier directement la personne concernée. Le résultat du traitement n'est conservé par l'UIP que le temps nécessaire pour informer les autorités nationales compétentes et pour informer les UIP des autres États membres de l'existence d'une concordance positive.

Les UIP ne traitent que les données énumérées à l'annexe I de la directive, aux fins:

- de réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités nationales compétentes et, si nécessaire, par Europol;

- de répondre, au cas par cas, aux demandes des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, et visant à communiquer à ces autorités compétentes ou, le cas échéant, à Europol le résultat de ce traitement;

- d'analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à appliquer en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

Lorsqu'elle réalise une telle évaluation, l'UIP peut soit confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données, soit traiter les données PNR au regard de critères préétablis. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Il revient aux UIP de fixer ces critères et de les réexaminer à intervalles réguliers en coopération avec les autorités compétentes concernées. Lesdits critères ne sont pas fondés sur des données à caractère personnel sensibles telles que l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

En ce qui concerne les personnes identifiées, les UIP transmettent toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données aux UIP correspondantes des autres États membres. Lesdites UIP transmettront les informations reçues à leurs propres autorités compétentes.

Le délégué à la protection des données nommé par l'UIP est chargé de contrôler le traitement des données PNR. La personne concernée a le droit de s'adresser au délégué à la protection des données, en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant.

Tous les transferts de données PNR effectués par des transporteurs aériens vers les UIP doivent être effectués par des moyens électroniques qui en assurent la sécurité sur le plan technique. À cet effet, tant les protocoles communs auxquels les transporteurs aériens doivent se conformer lorsqu'ils transfèrent les données que les formats de données reconnus qui en assure la lisibilité par toutes les parties concernées sont définis au niveau de l'UE[32].

---

[32] Décision d'exécution (UE) 2017/759 de la Commission du 28 avril 2017 sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers, JO L 113 du 29.4.2017, p. 48.

1.14. Points d'accès nationaux à l'EES

Le système d'entrée/de sortie (EES)[33] vise principalement à améliorer la gestion des frontières extérieures de l'Union et est utilisé à cet effet par les autorités frontalières, les autorités chargées de l'immigration et les autorités chargées des visas[34]. Le système enregistre de manière électronique l'heure et le lieu d'entrée et de sortie de certains ressortissants de pays tiers qui sont admis pour un court séjour sur le territoire des États membres et calcule la durée de leur séjour autorisé. L'EES est mis en œuvre aux frontières extérieures. Les États membres qui appliquent l'acquis de Schengen dans son intégralité introduisent l'EES à leurs frontières intérieures avec les États membres qui n'appliquent pas encore l'acquis de Schengen dans son intégralité mais qui mettent en œuvre ou non l'EES. Aucune fonctionnalité biométrique n'est mise en œuvre par les États membres qui n'appliquent pas l'acquis de Schengen dans son intégralité.

Outre les autorités frontalières, les autorités chargées de l'immigration et les autorités chargées des visas, l'EES peut être consulté par les "autorités nationales désignées" dans les conditions prévues par le règlement. Ces autorités désignées consultent l'EES à des fins répressives, et aussi pour permettre la production d'informations aux fins des enquêtes relatives à des infractions terroristes et à d'autres infractions pénales graves, y compris l'identification des auteurs et des personnes soupçonnées d'avoir commis de telles infractions ainsi que des victimes de telles infractions qui ont franchi les frontières extérieures.

Les États membres désignent les autorités habilitées à consulter l'EES à des fins répressives. Chaque État membre désigne en outre un point d'accès central à l'EES. Distinct des "autorités désignées", le point d'accès central accomplit ses missions en toute indépendance des "autorités désignées" et ne reçoit d'elles aucune instruction concernant le résultat de ses vérifications, c'est-à-dire le processus consistant à comparer des séries de données en vue d'établir la validité d'une identité déclarée, de manière à garantir que celui-ci est effectué de manière indépendante. Seul le personnel dûment habilité du points d'accès central est autorisé à accéder à l'EES.

---

33 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.

34 La Commission fixera la date à laquelle l'EES doit être mis en service, une fois que les conditions énoncées à l'article 66 du règlement (UE) 2017/2226 sont remplies.

Les unités opérationnelles au sein des "autorités désignées" sont autorisées à demander l'accès aux données de l'EES par l'intermédiaire des points d'accès centraux. À cette fin, l'unité opérationnelle doit présenter à un point d'accès central, sous forme électronique ou écrite, une demande motivée d'accès aux données de l'EES. Le point d'accès central vérifie si les conditions d'accès, définies dans le règlement, sont remplies et, si tel est le cas, traite la demande. Les données de l'EES seront ensuite communiquées à une unité opérationnelle selon des modalités qui ne compromettent pas la sécurité des données.

Les conditions qui doivent être examinées avant d'autoriser l'accès aux données de l'EES à des fins répressives sont les suivantes:

- l'accès en consultation est nécessaire à des fins répressives;
- l'accès en consultation est nécessaire et proportionné dans un cas spécifique;
- il existe des preuves ou des motifs raisonnables permettant de considérer que la consultation des données de l'EES contribuera à la prévention et à la détection de l'une des infractions pénales en question, ou aux enquêtes en la matière, en particulier lorsqu'il y a des motifs fondés permettant de croire que la personne soupçonnée d'avoir commis une infraction terroriste ou une autre infraction pénale grave, l'auteur ou la victime d'une telle infraction relève d'une catégorie couverte par le règlement.

En outre, l'accès à l'EES en tant qu'outil destiné à identifier une personne soupçonnée d'avoir commis de telles infractions, l'auteur ou la victime de telles infractions est autorisé lorsque:

- les bases de données nationales ont déjà été interrogées;
- dans le cas des recherches à l'aide d'empreintes digitales, une recherche préalable a été lancée au titre de la décision 2008/615/JAI du Conseil (décision Prüm), lorsque les comparaisons d'empreintes digitales sont disponibles techniquement, et cette recherche soit a été effectuée intégralement, soit n'a pas été effectuée intégralement dans les deux jours suivant son lancement.

Une demande de consultation du VIS au sujet de la même personne concernée peut être présentée parallèlement à une demande de consultation de l'EES, conformément aux conditions prévues dans la décision 2008/633/JAI du Conseil[35].

Enfin, l'accès à l'EES en tant qu'outil permettant de consulter l'historique des déplacements ou les périodes de séjour sur le territoire des États membres d'une personne connue soupçonnée d'avoir commis une infraction terroriste ou une autre infraction pénale grave, d'un auteur connu ou d'une personne connue présumée victime d'une telle infraction est autorisé lorsque les principes susmentionnés sont respectés.

1.15. Unités nationales ETIAS[36]

Le système européen d'information et d'autorisation concernant les voyages (ETIAS) soutient[37] l'échange d'informations aux fins de la gestion des frontières, du contrôle de l'application de la loi et de la lutte contre le terrorisme. L'ETIAS a pour objectif de déterminer si les ressortissants de pays tiers exemptés de l'obligation de visa remplissent les conditions applicables, préalablement à leur voyage vers l'espace Schengen et avant leur arrivée aux points de passage des frontières extérieures. L'ETIAS fournit une autorisation de voyage, qui est par nature différente d'un visa mais constitue une condition d'entrée et de séjour, et qui indique que le demandeur ne présente pas un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé.

L'ETIAS est composé:

- du système d'information ETIAS, y compris la liste de surveillance ETIAS;
- de l'unité centrale ETIAS, qui fait partie de l'Agence européenne de garde-frontières et de garde-côtes;
- des unités nationales ETIAS.

---

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

36 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.
Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), JO L 236 du 19.9.2018, p. 72.

37 La Commission fixera la date à laquelle l'ETIAS doit être mis en service, une fois que les conditions énoncées à l'article 88 du règlement (UE) 2018/1240 sont remplies.

Lorsque le traitement automatisé d'une demande fait apparaître une correspondance ("hit") entre les données enregistrées dans le dossier de demande et les données figurant dans le système d'information ETIAS, les indicateurs de risques spécifiques ou des signalements consignés dans les systèmes d'information de l'UE consultés, l'unité centrale ETIAS est chargée de vérifier cette correspondance et, si celle-ci est confirmée ou que des doutes subsistent, d'engager le traitement manuel de la demande dans l'État membre identifié.

C'est ensuite à l'unité nationale ETIAS de l'État membre concerné qu'il revient de traiter manuellement la demande en question. Celle-ci a accès au dossier de demande et à tout dossier de demande éventuel qui y est lié, ainsi qu'à toute réponse positive (hit) déclenchée pendant le traitement automatisé. À l'issue du traitement manuel, l'unité nationale responsable délivrera ou refusera, conformément aux dispositions du règlement, une autorisation de voyage. À cette fin, l'unité nationale peut demander des informations ou des documents supplémentaires.

Une autorisation de voyage doit être refusée si le demandeur:

- a utilisé un document de voyage signalé dans le SIS comme ayant été égaré, volé, détourné ou invalidé;
- présente un risque en matière de sécurité;
- présente un risque en matière d'immigration illégale;
- présente un risque épidémique élevé;
- fait l'objet d'un signalement dans le SIS aux fins de non-admission ou d'interdiction de séjour;
- ne répond pas à une demande d'informations ou de documents supplémentaires, ou ne se présente pas à un entretien.

Les unités nationales ETIAS sont chargées d'examiner les demandes et de décider de délivrer, de refuser, d'annuler ou de révoquer les autorisations de voyage. À cette fin, elles devraient coopérer entre elles ainsi qu'avec Europol aux fins de l'évaluation des demandes.

Une unité nationale peut décider de refuser ou d'annuler une autorisation de voyage s'il s'avère que les conditions requises n'étaient pas remplies au moment de sa délivrance, ou de révoquer une autorisation de voyage lorsqu'il s'avère que les conditions de délivrance ne sont plus remplies. Les demandeurs concernés ont le droit d'introduire un recours. Les recours doivent être intentés dans l'État membre qui s'est prononcé sur le refus, l'annulation ou la révocation, et conformément au droit national de cet État membre. L'unité nationale compétente est chargée de fournir aux demandeurs des informations concernant la procédure de recours.

Les autorités frontalières compétentes pour effectuer les vérifications aux points de passage des frontières extérieures consultent le système central ETIAS en utilisant les données intégrées dans la bande de lecture optique du document de voyage. Les autorités chargées de l'immigration qui contrôlent ou vérifient si les conditions d'entrée ou de séjour sur le territoire des États membres sont remplies peuvent accéder au système central ETIAS afin d'y effectuer des recherches.

Uniquement dans des cas spécifiques et pour autant que cela soit nécessaire aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, et aux fins des enquêtes en la matière, les autorités répressives désignées par les États membres sont habilitées à demander la consultation des données à caractère personnel enregistrées dans le système central ETIAS. La directive (UE) 2016/680 (directive "police" relative à la protection des données) s'applique au traitement de ces données à caractère personnel par les autorités désignées des États membres en application du règlement ETIAS.

1.16. Interopérabilité

Le "train de mesures sur l'interopérabilité"[38] a pour principal objectif d'améliorer l'architecture de gestion des données mise en place par l'Union pour la gestion des frontières et la sécurité en vue de faciliter l'identification correcte des personnes qui ne sont pas des citoyens européens mais des ressortissants de pays tiers. L'interopérabilité entre l'EES (voir point 3.19), le VIS (voir point 3.8), l'ETIAS (voir point 3.20), Eurodac (voir point 3.9), le SIS (voir point 3.3) et l'ECRIS-TCN (voir point 3.14.1) vise à permettre à ces systèmes d'information de l'UE de se compléter mutuellement. À cet effet, il convient de créer un portail de recherche européen (ESP), un service partagé d'établissement de correspondances biométriques (BMS partagé), un répertoire commun de données d'identité (CIR) et un détecteur d'identités multiples (MID)[39].

a) Afin d'assurer l'utilisation systématique des systèmes d'information de l'UE susmentionnés, les autorités désignées habilitées à avoir accès à au moins un de ces systèmes d'information, au CIR et au MID, ainsi qu'aux données Europol ou aux bases de données d'Interpol SLTD et TDAWN (voir point 2.4), devraient utiliser l'ESP, qui permet d'interroger simultanément ces systèmes d'information.

b) Le répertoire commun de données d'identité (CIR) crée un dossier individuel pour chaque personne enregistrée dans les systèmes d'information en question et est conçu comme un réservoir partagé pour les données d'identité, les données du document de voyage et les données biométriques des personnes enregistrées dans ces systèmes. Le CIR devrait faire partie de l'architecture technique de ces systèmes et constituer l'élément partagé entre ceux-ci pour stocker et interroger les données d'identité, les données relatives aux voyages et les données biométriques qu'ils traitent.

---

[38] 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, JO L 135 du 22.5.2019, p. 27.
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, JO L 135 du 22.5.2019, p. 85.

[39] La Commission fixera la date à partir de laquelle s'appliqueront les dispositions des règlements relatives à l'ESP, au BMS partagé, au CIR et au MID.

L'accès au CIR est accordé notamment aux fins suivantes:

- faciliter l'identification correcte des personnes enregistrées dans les systèmes d'information de l'UE ou, si nécessaire,

- aider les autorités répressives à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière.

Lorsque, pour différentes raisons, un service de police n'est pas en mesure d'identifier une personne, celui-ci peut interroger le CIR. À cette fin, les États membres habilitent, sur la base de leur législation nationale, les services compétents à procéder à cette interrogation et fixent les procédures, les conditions et les critères relatifs à ces contrôles. L'interrogation du CIR est effectuée sur la base d'empreintes digitales récemment prélevées sur la personne concernée ou, lorsque la requête introduite avec ces données échoue, à l'aide des données d'identité de cette personne, combinées aux données du document de voyage.

Dans le cas où le résultat de l'interrogation indiquerait que des données concernant cette personne sont stockées dans le CIR, le service de police compétent obtiendra le nom de famille, le ou les prénoms, le lieu de naissance, la date de naissance, la nationalité, le genre, les noms utilisés antérieurement, le cas échéant, les éventuels pseudonymes, ainsi que, si elles dont disponibles, des informations sur les documents de voyage. En outre, un service de police peut, s'il y est habilité par la législation nationale, interroger le CIR à l'aide de données biométriques en cas de catastrophe naturelle, d'accident ou d'attaque terroriste, et uniquement aux fins d'identification de personnes inconnues qui ne sont pas en mesure de s'identifier elles-mêmes ou de restes humains non identifiés.

Lorsqu'elles interrogent le CIR à des fins répressives, notamment lorsqu'il y a lieu de penser que la personne soupçonnée d'avoir commis une infraction terroriste ou une autre infraction pénale grave, ou l'auteur ou la victime d'une telle infraction est une personne dont les données sont stockées dans les systèmes d'information, les autorités désignées et Europol peuvent consulter le CIR pour savoir si des données sur une personne en particulier sont stockées. Si tel est le cas, le CIR fournit, après la vérification automatisée de la présence d'une correspondance dans le système (fonctionnalité dite de l'indicateur de correspondance), une réponse sous la forme d'une référence indiquant le système d'information qui contient des données correspondantes. La réponse induite par l'indicateur de correspondance ne devrait être utilisée qu'aux fins de l'introduction d'une demande d'accès au système d'information de l'UE sous-jacent. Une telle réponse ne devrait pas révéler les données à caractère personnel de la personne concernée, mais seulement indiquer que des données la concernant sont stockées dans l'un des systèmes.

L'utilisateur final autorisé ne devrait prendre aucune décision défavorable à l'égard de la personne concernée en se fondant uniquement sur l'existence d'un indicateur de correspondance. L'accès de l'utilisateur final à un indicateur de correspondance est dès lors supposé constituer une atteinte très limitée au droit à la protection des données à caractère personnel de la personne concernée, tout en permettant aux autorités désignées de demander l'accès aux données à caractère personnel de manière plus efficace. L'accès complet aux données à des fins répressives reste soumis aux conditions et procédures prévues dans le règlement Eurodac (voir point 2.7).

c) Le détecteur d'identités multiples (MID) crée et stocke des liens entre les données contenues dans les différents systèmes d'information de l'UE. En matière répressive, une détection d'identités multiples dans le CIR et le SIS est lancée lorsqu'un signalement concernant une personne est créé ou mis à jour dans le SIS, ou lorsqu'un fichier de données est créé ou modifié dans l'ECRIS-TCN. La détection d'identités multiples est lancée uniquement pour comparer les données disponibles dans un système d'information de l'UE à celles qui sont disponibles dans un autre système d'information de l'UE. La vérification des différentes identités est effectuée manuellement soit par le bureau SIRENE compétent, soit par les autorités centrales concernées.

La Commission:

- fixera la date à partir de laquelle s'appliqueront les dispositions des règlements relatives à l'ESP, au BMS partagé, au CIR et au MID;

- en étroite coopération avec les États membres, l'eu-LISA et les autres agences de l'Union concernées, mettra à disposition un manuel pratique sur la mise en œuvre et la gestion des éléments d'interopérabilité. Le manuel pratique contient des orientations techniques et opérationnelles, des recommandations et des bonnes pratiques.

1.17. Choix du canal - Critères communément utilisés

Dans un État membre, le PCU[40] joue un rôle essentiel dans la détermination du canal le plus approprié et le plus pertinent pour rassembler toutes les demandes (à la fois entrantes et sortantes) traitées par l'unité. Au nom de l'efficacité, les autorités nationales laissent une très grande autonomie aux enquêteurs pour choisir le canal censé être le mieux adapté à l'enquête. Les canaux de communication les plus couramment utilisés sont les suivants:

- SIRENE par l'intermédiaire des points de contact dans chaque État Schengen pour le SIS;
- EUROPOL par l'intermédiaire des unités nationales d'Europol / des officiers de liaison Europol;
- INTERPOL par l'intermédiaire des bureaux centraux nationaux présents aux sièges des polices nationales;
- des officiers de liaison;
- les canaux d'assistance mutuelle utilisés entre autorités douanières (Naples II);
- des canaux bilatéraux fondés sur des accords de coopération aux niveaux national, régional et local (CCPD).

La règle veut, de manière générale, que les demandes ne soient transmises que par un seul canal. Toutefois, une demande peut, dans des circonstances exceptionnelles, être transmise par plusieurs canaux à la fois. Dans ce cas, il convient de l'indiquer clairement à toutes les parties de manière appropriée. De même, tout changement de canal doit être communiqué à l'ensemble des parties et être motivé.

Afin d'éviter des chevauchements thématiques ou des situations dans lesquelles une demande est inutilement transmise à plusieurs reprises par des canaux différents, l'administrateur compétent (SIS, Europol, Interpol, un officier de liaison bilatéral) dans l'État requérant peut déterminer le meilleur parcours pour une demande d'informations sur la base des critères suivants:

---

[40] Lignes directrices concernant un PCU, doc. 10492/14 DAPIX 75 ENFOPOL 157 et 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

- des critères géographiques, c'est-à-dire lorsque la nationalité, le lieu de résidence ou le lieu d'origine de la personne ou de l'objet concernés sont connus et que la demande porte sur la communication de données (adresse, numéro de téléphone, empreintes digitales, ADN, immatriculation, etc.);

- des critères thématiques, c'est-à-dire concernant le thème (criminalité organisée, infractions graves, terrorisme), le caractère confidentiel ou sensible des informations et le canal utilisé pour une demande antérieure similaire;

- des critères techniques, c'est-à-dire portant sur la nécessité de disposer de canaux informatiques sécurisés;

- des critères d'urgence, c'est-à-dire dans les cas de risque immédiat pour l'intégrité physique des personnes, de perte immédiate d'éléments de preuve, de demande d'opérations transfrontières ou de surveillance urgentes.

2. SYSTEMES D'INFORMATION

2.1. Système d'information Schengen – Deuxième génération (SIS II)[41]

Actuellement, le système d'information Schengen de deuxième génération ("SIS II") est opérationnel dans 26 États membres de l'UE, ainsi que dans les quatre pays tiers qui sont associés à la coopération Schengen: la Norvège, l'Islande, la Suisse et le Liechtenstein. Il apporte un soutien à la coopération opérationnelle en matière pénale entre les services de police et les autorités judiciaires. Le SIS étant à la fois un système de coopération policière et de contrôle aux frontières, les fonctionnaires de police, gardes-frontières et agents des douanes désignés ainsi que les autorités judiciaires et chargées des visas dans l'ensemble de l'espace Schengen peuvent consulter le SIS[42].

Les données du SIS II peuvent être consultées (sous réserve du respect de règles strictes en matière de protection des données) 24 heures sur 24 et 7 jours sur 7 par l'intermédiaire de points d'accès dans les bureaux SIRENE et des points de contrôle des frontières, sur le territoire national et auprès des consulats à l'étranger. La base de données conserve des données tant sur les **personnes** et les **objets** et permet l'échange de données aux fins de la prévention de la criminalité et de la lutte contre l'immigration clandestine. Par des consultations du SIS effectuées en ligne, l'agent chargé de l'examen établit rapidement, la base d'un système "hit - no hit", si la personne contrôlée figure ou non dans la base de données.

---

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

42 Une liste des autorités nationales compétentes qui disposent d'un droit d'accès aux signalements est publiée chaque année au *Journal officiel de l'Union européenne*.

Les données prennent la forme de signalements qui ne contiennent que les informations nécessaires à l'identification d'une personne ou d'un objet et pour déterminer les mesures à prendre. Le réseau unique des bureaux Sirene nationaux assure l'échange d'informations supplémentaires conformément aux dispositions du manuel Sirene. Un signalement est un ensemble de données qui permettent aux autorités d'identifier des personnes ou des objets en vue de prendre les mesures appropriées.

Il peut s'agir de signalements concernant des personnes, ciblant à la fois des citoyens de l'UE et des ressortissants de pays tiers. Ces signalement facilitent la prise de mesures telles que:

– une arrestation aux fins de remise sur la base soit d'un mandat d'arrêt européen soit d'accords conclus entre l'UE et des pays tiers, ou aux fins d'extradition;

– une recherche aux fins de localisation de personnes disparues;

– des citations à comparaître devant un tribunal dans le cadre d'une procédure pénale ou de l'exécution d'une peine privative de liberté;

– une surveillance discrète et des contrôles spécifiques en vue de réprimer des infractions pénales ou de prévenir des menaces contre la sécurité publique ou la sécurité nationale;

– une non-admission dans l'espace Schengen de ressortissants nationaux ou étrangers à la suite d'une décision administrative ou judiciaire ou par des raisons de menace pour l'ordre public, la sûreté nationale et la sécurité intérieure, ou pour non-respect des réglementations nationales en matière d'entrée et de séjour des étrangers.

Les signalements SIS II concernant des **objets** sont introduits aux fins de surveillance discrète ou de contrôles spécifiques, à des fins de saisie, d'utilisation comme preuve dans une procédure pénale ou de surveillance. Ces signalements peuvent porter sur:

– des véhicules, des bateaux, des aéronefs, des conteneurs,

– des armes à feu,

– des documents volés,

– des billets de banque,

– des biens volés tels que des œuvres d'art, des bateaux ou de navires.

Plus précisément, le personnel autorisé d'Europol a le droit, dans les limites de son mandat, d'accéder aux données introduites dans le SIS II et de les consulter directement, et il peut demander des informations supplémentaires à l'État membre concerné.

Les membres nationaux d'Eurojust et leurs assistants ont le droit, dans les limites de leur mandat, d'accéder aux données introduites dans le SIS II et de les consulter.

Trois ans après la mise en service du SIS II, la Commission a procédé à une évaluation du système. Les trois nouveaux règlements SIS récemment adoptés (refonte du SIS) tiennent compte de cette évaluation et visent à accroître l'efficacité de la lutte contre le terrorisme et les formes graves de criminalité, notamment par un meilleur échange d'informations entre les autorités compétentes. Ces règlements contribuent en outre à la gestion des frontières et des migrations et préparent l'interopérabilité du SIS avec les systèmes d'information à grande échelle de l'UE, tels que le VIS, Eurodac, l'ETIAS et l'EES. Les règlements modifiant le cadre juridique et opérationnel du SIS II sont les suivants:

- règlement (UE) 2018/1860 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier[43];

- règlement (UE) 2018/1861 sur l'établissement, le fonctionnement et l'utilisation du SIS dans le domaine des vérifications aux frontières[44]; et

- règlement (UE) 2018/1862 sur l'établissement, le fonctionnement et l'utilisation du SIS dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale[45];

---

43 Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).

44 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).

45 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).

Les trois règlements SIS révisés sont entrés en vigueur en décembre 2019 et seront pleinement opérationnels à partir de décembre 2021. Les nouvelles fonctionnalités du SIS sont mises en œuvre en différentes étapes, les travaux devant être achevés d'ici 2021. Un système automatisé d'identification par empreintes digitales (AFIS) a été introduit dans le SIS en mars 2018, ce qui permettra d'effectuer des recherches à l'aide des empreintes digitales à partir de 2021.

Les règlements contiennent des règles spécifiques concernant les États membres qui ont un statut particulier pour ce qui est de Schengen et des mesures relatives à l'espace de liberté, de sécurité et de justice adoptées dans le cadre du TFUE, à savoir le Danemark, l'Irlande, la Croatie, la Bulgarie, la Roumanie et Chypre. En outre, le règlement (UE) 2018/1861 et le règlement (UE) 2018/1860 fournissent la base juridique permettant aux membres d'une équipe du corps européen de garde-frontières et de garde-côtes d'avoir directement accès aux données du SIS aux fins des vérifications aux frontières et du retour des ressortissants de pays tiers en séjour irrégulier. Dans le cadre de leur mandat et à condition qu'ils soient autorisés à effectuer des vérifications et aient reçu la formation requise, les membres de l'équipe du corps européen de garde-frontières et de garde-côtes exerceront ce droit au moyen d'une interface technique, qui doit être mise en place et gérée par l'Agence européenne de garde-frontières et de garde-côtes (Frontex) et permettra une connexion directe au SIS II central.

2.2. SIE - Système d'information Europol[46]

Le règlement Europol introduit un nouveau concept pour le traitement des données, communément appelé le concept de gestion intégrée des données ("Integrated Data Management Concept"). Ce concept peut être défini comme étant la possibilité d'utiliser des informations relatives à des activités criminelles afin de les exploiter de diverses manières conformément à ce qu'a indiqué le propriétaire des données, ce qui permet de les gérer et de les traiter d'une manière intégrée technologiquement neutre. En vertu de la décision du Conseil portant création d'Europol, le traitement des données s'articulait autour de systèmes. Le règlement Europol ne contient plus de références à des systèmes mais requiert d'indiquer à quelles fins les données sont traitées. Afin de faciliter une transition en douceur, les utilisateurs peuvent continuer à travailler avec les systèmes existants en le faisant d'une manière conforme au nouveau cadre juridique.

---

[46] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à partir du 1er mai 2017).

Le système d'information Europol (SIE), mentionné dans la décision Europol, est un système centralisé hébergé par Europol qui permet aux États membres et aux partenaires de coopération d'Europol de stocker, de partager et de recouper les données relatives à des suspects, à des personnes condamnées ou à des "futurs délinquants potentiels" impliqués dans des activités criminelles relevant du mandat d'Europol (infractions graves, criminalité organisée ou terrorisme). Il permet le stockage de tout l'éventail des données et des éléments de preuve en rapport avec ces activités criminelles/ces personnes, comme par exemple des personnes ayant des pseudonymes, des sociétés, des numéros de téléphone, des adresses de courrier électronique, des véhicules, des armes à feu, des échantillons d'ADN, des photos, des empreintes digitales, des bombes, etc. Le SIE, qui sert avant tout de système facilitant les recoupements, fournit un accès fondé sur un système de concordance/non-concordance. Le règlement Europol prévoit un accès total aux données transmises pour une analyse de nature stratégique ou thématique mais seulement un accès fondé sur un critère de concordance/non-concordance aux données fournies pour une analyse opérationnelle.

Le SIE est de facto un système de référence qui aide à déterminer si les informations recherchées sont disponibles dans un des États membres de l'UE, auprès de partenaires de coopération ou au sein d'Europol. Il est directement accessible dans tous les États membres ainsi qu'au personnel d'Europol dûment habilité. Actuellement, on peut distinguer trois méthodes par lesquelles les États membres chargent les données:

a) introduction manuelle des données dans le SIE ou par l'intermédiaire de SIENA;

b) transfert semi-automatisé en effectuant un chargement par lots dans le SIE;

c) transfert automatisé à l'aide d'un chargeur de données.

La grande majorité des données figurant dans le système d'information Europol (SIE) sont introduites au moyen de systèmes de chargement automatique de données. L'approche des États membres en matière de collecte de données a changé, l'accent en matière de transmission de données étant déplacé vers des éléments pouvant faire l'objet de recoupements, tels que des personnes, des voitures, des numéros de téléphone et des armes à feu.

Les pays tiers ne peuvent pas directement introduire ni recouper des données dans le SIE mais, conformément à l'article 23, paragraphe 5, du règlement Europol, ils peuvent les envoyer à Europol. Europol devra d'abord évaluer si les données relèvent bien de son mandat avant de les accepter et d'effectuer le recoupement de ces données.

Le SIE, qui permet le partage d'informations très sensibles, est doté d'un solide système garantissant la confidentialité et la sécurité. La sécurité est assurée, par exemple, par les codes de traitement spécifiques. Ceux-ci indiquent ce qu'il est possible de faire avec les informations données ainsi que qui y a accès. Les codes de traitement sont conçus pour protéger la source d'information et assurer que le traitement des informations s'effectue conformément aux souhaits du propriétaire de ces informations et à la législation nationale de l'État membre. Le SIE est homologué pour le traitement de données jusqu'au niveau "RESTREINT UE/EU RESTRICTED" compris.

2.3. SIENA - Application de réseau d'échange sécurisé d'informations d'Europol

SIENA est le système de communication sécurisé d'Europol visant à permettre aux États membres, à Europol et à ses partenaires de coopération d'échanger des informations et des renseignements opérationnels et stratégiques liés à la criminalité, y compris des données opérationnelles concernant les personnes. SIENA est un système de messagerie proposant différents types de messages à des fins variées, y compris pour l'échange de données conformément à la "décision-cadre suédoise".

Dans la conception et le fonctionnement de SIENA, un accent tout particulier a été mis sur la sécurité, la protection des données et la confidentialité. SIENA a été homologué pour l'échange d'informations de niveau "CONFIDENTIEL UE/EU CONFIDENTIAL". L'échange de données au moyen de SIENA implique des responsabilités claires en matière de traitement des données. Pour chaque message SIENA envoyé, la classification (confidentialité), les codes de traitement et la fiabilité de la source et des informations doivent être indiqués.

La langue par défaut de l'interface utilisateur de SIENA est l'anglais, tandis que l'interface est plurilingue, permettant ainsi aux opérateurs SIENA de travailler dans leur(s) propre langue(s) nationale(s). En plus d'échanger des messages, les opérateurs SIENA peuvent effectuer des recherches et créer des rapports statistiques sur les données échangées par l'intermédiaire de SIENA.

SIENA facilite l'échange bilatéral de données entre les États membres et leur permet d'échanger des données en dehors du mandat d'Europol. Lorsqu'ils s'adressent à l'un des partenaires de coopération d'Europol dans l'échange de données, les États membres sont informés, par l'intermédiaire de SIENA, que cet échange ne devrait avoir lieu que s'il concerne des infractions relevant du mandat d'Europol.

Europol ne traite les informations échangées au moyen de SIENA à des fins de traitement des données opérationnelles que si Europol est inclus en tant que destinataire de l'échange de données. À des fins d'audit, toutes les données échangées par l'intermédiaire de SIENA sont à la disposition du délégué à la protection des données d'Europol et des organismes de contrôle nationaux.

SIENA facilite l'échange structuré de données qui s'appuient sur le format universel pour les messages (UMF). Actuellement, l'entité UMF PERSON peut être créée/affichée dans l'application web SIENA proprement dite. Le modèle de données UMF complet est déjà pris en charge par le service web SIENA.

2.4. I-24/7 - Système mondial de communication policière d'Interpol

Le réseau mondial d'échange d'informations policières I-24/7 est relié aux Secrétariat d'Interpol à Lyon (France), aux bureaux centraux nationaux (BCN) dans 190 pays et à des bureaux régionaux.

Le système d'information d'Interpol permet la communication directe par messages entre les BCN. Toutes les bases de données d'Interpol (à l'exception de la base de données d'images en matière d'exploitation sexuelle des enfants) sont accessibles en temps réel par l'intermédiaire du système mondial de communication policière I-24/7. Le système I-24/7 permet aussi aux pays membres d'accéder aux bases de données nationales les uns des autres en utilisant une connexion interentreprises (B2B). Les États membres gèrent et mettent à jour leurs propres données pénales nationales et en contrôlent la soumission, l'accès par d'autres pays et de la destruction de données conformément à leur législation nationale. Ils ont également la possibilité de les rendre accessibles à la communauté internationale des services répressifs par l'intermédiaire du système I-24/7.

2.4.1. Interpol: Passerelle ADN

La base de données ADN d'Interpol contient une base de données ADN internationale, un formulaire de demande de recherche internationale pour l'échange bilatéral et un moyen de transmission électronique normalisée et sécurisée. Aucune donnée nominative n'est conservée reliant un profil ADN à un individu. La passerelle ADN est compatible avec l'échange automatisé de données dans le cadre de Prüm.

Les pays membres peuvent accéder à la base de données et, sur demande, l'accès peut être étendu au-delà des bureaux centraux nationaux des pays membres jusqu'à comprendre les centres et laboratoires de police scientifique. La police des pays membres peut soumettre un profil ADN provenant de délinquants, de scènes de crime, de personnes disparues et de cadavres non identifiés.

2.4.2. Base de données d'empreintes digitales d'Interpol

Les utilisateurs autorisés dans les pays membres peuvent visualiser et soumettre des relevés et procéder à leur vérification croisée au moyen d'un système de reconnaissance automatisée d'empreintes digitales (AFIS). Les relevés sont conservés et échangés dans le format défini par l'Institut national des normes et des technologies (NIST). Les lignes directrices concernant la transmission des empreintes digitales et les lignes directrices concernant la transmission des empreintes digitales retrouvées sur les scènes de crime, aident les États membres à améliorer la qualité et la quantité des relevés d'empreintes digitales transmis au système AFIS d'Interpol.

2.4.3. Base de données d'Interpol sur les documents de voyage volés ou perdus

La base de données d'Interpol sur les documents de voyage volés ou perdus contient des informations sur plus de 45 millions de documents de voyage déclarés perdus ou volés par 166 pays. Cette base de données permet aux BCN Interpol et aux membres d'autres services répressifs autorisés (tels que les agents de l'immigration et du contrôle aux frontières) de vérifier la validité d'un document de voyage suspect. Aux fins de prévenir et de combattre la grande criminalité et la criminalité organisée, les services répressifs compétents des États membres échangent des données relatives aux passeports avec Interpol[47].

2.4.4. Documents de voyage associés aux notices (TDAWN)

La base de données concernant les documents de voyage associés aux notices (TDAWN) contient des informations sur les documents de voyage liés à des personnes faisant l'objet d'une notice d'Interpol.

2.4.5. Tableau de référence des armes à feu

Le tableau de référence INTERPOL des armes à feu permet aux enquêteurs d'identifier convenablement une arme à feu utilisées lors d'une infraction (marque, modèle, calibre, etc.). Il contient plus de 250 000 références d'armes à feu et 57 000 images de haute qualité. Le réseau d'information balistique d'INTERPOL est une plateforme pour le partage et la comparaison de données balistiques au niveau international et à grande échelle et il comporte plus de 150 000 entrées.

Le système INTERPOL de gestion des données sur les armes illicites et du traçage des armes (iARMS) est une application informatique qui facilite l'échange d'informations et la coopération entre les services répressifs en matière de criminalité liée aux armes à feu.

---

[47] Position commune 2005/69/JAI du Conseil du 24 janvier 2005 relative à l'échange de certaines données avec Interpol, JO L 27 du 29.1.2005, p. 61.

2.5. ECRIS[48]

Le système informatisé européen d'information sur les casiers judiciaires (ECRIS)[49] fournit des moyens électroniques permettant l'échange d'informations sur les condamnations entre États membres dans un format normalisé. Le système ECRIS est utilisé pour informer les États membres des condamnations de leurs ressortissants et envoyer des demandes d'informations sur les condamnations à des fins de procédure pénale et à d'autres fins, notamment administratives ou liées à l'emploi. Il est également possible d'introduire des demandes concernant des ressortissants de pays tiers, s'il y a des raisons de penser que l'État membre requis détient des informations concernant cette personne.

Les demandes ECRIS doivent recevoir une réponse dans les 10 jours ouvrables, si la demande a été introduite à des fins de procédure pénale ou pour des raisons liées à l'emploi, et dans un délai de 20 jours ouvrables si la demande émane d'une personne pour sa propre information.

Le système ECRIS n'est pas conçu pour devenir une base de données centralisée des casiers judiciaires et il s'appuie sur une architecture informatique décentralisée dans le cadre de laquelle tous les casiers judiciaires ne sont conservés que dans des bases de données gérées par les États membres. Les données sont échangées par voie électronique entre les autorités centrales désignées des États membres.

Les informations doivent être transmises par les États membres conformément aux règles convenues et dans les formats normalisés, et elles doivent être aussi complètes que possible, de manière à permettre à l'État membre de réception de traiter les informations correctement et d'identifier la personne concernée. Les messages sont envoyés dans les langues officielles des États membres concernés ou dans une autre langue acceptée par les deux États membres.

---

48 Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, JO L 93 du 7.4.2009, p. 23.

49 Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil, JO L 151 du 7.6.2019, p. 143.

Un manuel non contraignant à l'intention des praticiens, qui fixe les procédures pour les échanges d'informations et en coordonne l'action aux fins du développement du système ECRIS et de son fonctionnement, est publié par le Secrétariat général du Conseil et mis à disposition en format électronique sur le site web du Conseil ainsi que sur le site web CIRCABC hébergé par la Commission européenne à l'adresse https://circabc.europa.eu. Les demandes d'accès au manuel devraient être adressées au Secrétariat du Conseil. Les demandes d'accès au groupe d'intérêts restreints "ECRIS Business and Technical Support" (soutien professionnel et technique ECRIS) devraient être adressées à la Commission européenne.

2.5.1. ECRIS-TCN[50]

Le cadre juridique de l'ECRIS ne répond pas suffisamment aux particularités des demandes concernant des ressortissants de pays tiers. Au sein de l'Union, les informations relatives aux ressortissants de pays tiers ne sont pas rassemblées, comme c'est le cas pour les ressortissants des États membres, dans l'État membre de nationalité, mais seulement conservées dans les États membres où les condamnations ont été prononcées. Grâce à l'ECRIS-TCN[51], l'autorité centrale d'un État membre peut déterminer quels autres États membres détiennent des informations sur le casier judiciaire d'un ressortissant d'un pays tiers. Le cadre de l'ECRIS peut ensuite être utilisé pour demander de telles informations à ces États membres, conformément à la décision-cadre 2009/315/JAI.

Le règlement définit les règles relatives à la création, au niveau de l'Union, d'un système centralisé contenant des données à caractère personnel, ainsi que les règles relatives à la répartition des responsabilités entre l'État membre et l'organisme responsable du développement et de la maintenance du système centralisé. Il garantit un niveau global approprié de protection et de sécurité des données, ainsi que la protection des droits fondamentaux des personnes concernées.

---

50 Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726, JO L 135 du 22.5.2019, p. 1. Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil, JO L 151 du 7.6.2019, p. 143.

51 La Commission fixera la date à laquelle l'ECRIS-TCN doit être mis en service, une fois que les conditions énoncées à l'article 35 du règlement (UE) 2019/816 sont remplies.

Les États membres devraient créer, dans l'ECRIS-TCN, des enregistrements concernant les ressortissants de pays tiers condamnés. Cela devrait se faire, si possible, automatiquement et sans retard injustifié après l'inscription de la condamnation dans le casier judiciaire national. Les États membres devraient, conformément au règlement, inscrire dans le système central les données alphanumériques et dactyloscopiques liées aux condamnations prononcées après la date de début d'inscription des données dans le système ECRIS-TCN. À partir de la même date, et à tout moment par la suite, les États membres devraient pouvoir saisir des images faciales dans le système central.

L'ECRIS-TCN permet le traitement de données dactyloscopiques aux fins d'identifier les États membres détenant des informations sur le casier judiciaire d'un ressortissant d'un pays tiers. Il devrait aussi permettre le traitement d'images faciales en vue de confirmer son identité. Il est essentiel que l'inscription et l'utilisation de données dactyloscopiques et d'images faciales n'excèdent pas ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, respectent les droits fondamentaux, de même que l'intérêt supérieur de l'enfant, et soient en conformité avec les règles applicables de l'Union en matière de protection des données.

Eurojust, Europol et le Parquet européen devraient avoir accès au système ECRIS-TCN pour identifier les États membres détenant des informations sur le casier judiciaire d'un ressortissant d'un pays tiers aux fins de l'accomplissement de leurs missions statutaires.

L'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) est chargée de développer et d'exploiter l'ECRIS-TCN.

2.6. Système d'information sur les visas (VIS)[52]

Le système d'information sur les visas (VIS) est principalement un système de contrôle de l'immigration. Il s'agit d'un outil servant à faciliter la consultation au niveau des consulats ainsi que les contrôles aux frontières par la vérification et l'échange électroniques de données sur les visas entre les États membres. En tant que tel, il cible les ressortissants étrangers soumis à l'obligation de visa. Les autorités désignées des États membres (c'est-à-dire les postes consulaires, les points de passage frontaliers, les autorités policières et les services de l'immigration)[53] et Europol[54], dans le cadre de ses tâches, sont autorisées à consulter le VIS[55] aux fins de la prévention, de la détection et de l'investigation:

- des infractions terroristes, c'est-à-dire des infractions définies par le droit national qui correspondent ou sont équivalentes aux infractions visées aux articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme; et

- des infractions pénales graves, c'est-à-dire des formes de criminalité qui correspondent ou sont équivalentes à celles visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI ("mandat d'arrêt européen").

---

52 Décision 2004/512/CE du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS), JO L 213 du 15.6.2004, p. 5

53 Liste des autorités compétentes dont le personnel dûment autorisé sera habilité à saisir, à modifier, à effacer ou à consulter des données dans le système d'information sur les visas (VIS), (2016/C 187/04), JO C 187 du 26.5.2016, p. 4.

54 Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 218 du 13.8.2008, p. 129; décision 2013/392/UE du Conseil fixant la date de prise d'effet de la décision 2008/633/JAI concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 198 du 23.7.2013, p. 45.

55 Le 16 avril 2015, la Cour de justice de l'Union européenne a annulé la décision 2013/392/UE du Conseil fixant la date de prise d'effet de la décision 2008/633/JAI concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. Toutefois, la Cour a déclaré que les effets de la décision 2013/392 seraient maintenus jusqu'à l'entrée en vigueur d'un nouvel acte appelé à la remplacer.

Conformément à la décision-cadre suédoise, les informations contenues dans le VIS peuvent être communiquées au Royaume-Uni et à l'Irlande par les autorités compétentes des États membres dont les autorités désignées ont accès au VIS, et les informations tenues dans les registres nationaux relatifs aux visas du Royaume-Uni et de l'Irlande peuvent être transmises aux services répressifs compétents des autres États membres.

Le VIS s'appuie sur une architecture centralisée et sur une plateforme commune avec le SIS II. Les données du VIS sont traitées en deux étapes. Dans un premier temps, les données traitées comprennent les données alphanumériques et les photos. Dans un deuxième temps, les données biométriques et les documents scannés sont traités et introduits dans le VIS. Le VIS comprend des données concernant les demandes de visa, des photographies, des empreintes digitales, des décisions connexes prises par les autorités chargées des visas et des liens entre des demandes connexes. Le VIS a recours à un système d'établissement de correspondances biométriques visant à garantir la fiabilité des comparaisons d'empreintes digitales à des fins:

- de vérification, c'est-à-dire de contrôle si les empreintes digitales scannées au point de passage frontalier correspondent à celles de la signalétique biométrique du visa, ou
- d'identification, c'est-à-dire de comparaison des empreintes digitales prises au point de passage frontalier avec le contenu de la base de données complète.

D'un point de vue technique, le VIS comporte trois niveaux: le niveau central, le niveau national et le niveau local, ce dernier incluant les postes consulaires, les points de passages frontaliers, les services de l'immigration et les services de police.
En mai 2018, la Commission a présenté une proposition législative modifiant le règlement VIS qui vise notamment à assurer l'interopérabilité entre d'autres bases de données dans le domaine de la justice et des affaires intérieures. La version améliorée du VIS ne devrait pas être opérationnelle avant la fin de 2021.

2.7. Eurodac[56] [57]

Eurodac aidait initialement à déterminer l'État membre responsable de l'examen des demandes d'asile présentées dans l'un des États membres, et, par ailleurs, à faciliter l'application de la convention de Dublin. L'accès à Eurodac à des fins de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes en la matière, n'est accordé que dans des cas bien déterminés.

Le règlement Eurodac n° 603/2013 fixe des règles concernant la transmission de données dactyloscopiques à l'unité centrale, l'enregistrement de ces données et d'autres données pertinentes dans la base de données centrale, leur conservation, leur comparaison avec d'autres données dactyloscopiques, la transmission des résultats de cette comparaison et le verrouillage et l'effacement des données enregistrées.

L'architecture du système Eurodac consiste a) en une base de données dactyloscopiques informatisée centrale ("système central") comprenant une unité centrale et un plan et un système de maintien des activités, et b) en une infrastructure de communication entre le système central et les États membres, qui fournit un réseau virtuel crypté consacré aux données d'Eurodac ("infrastructure de communication").

Chaque État membre dispose d'un seul point d'accès national.

---

56 Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système "Eurodac" pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, JO L 316 du 15.12.2000, p. 1.

57 Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte).

L'agence eu-LISA instituée par le règlement (UE) n° 1077/2011[58] est chargée de la gestion opérationnelle d'Eurodac, et veille, en coopération avec les États membres, à ce que le système central bénéficie à tout moment des meilleures et des plus sûres techniques et technologie disponibles, sous réserve d'une analyse coût-bénéfice.

Tout État membre peut transmettre des empreintes digitales à l'unité centrale en vue de vérifier si un étranger d'au moins 14 ans se trouvant illégalement sur son territoire a déjà introduit une demande d'asile dans un autre État membre. L'unité centrale compare ces empreintes digitales avec les données dactyloscopiques transmises par d'autres États membres et déjà conservées dans la base de données centrale. L'unité informe l'État membre qui a transmis les données pour savoir s'il y a eu une correspondance, c'est-à-dire si la comparaison entre les empreintes digitales enregistrées et transmises a donné un résultat positif. Cet État membre vérifie le résultat et procède à l'identification définitive en coopération avec les États membres concernés.

Les États membres sont tenus de veiller à la régularité, à l'exactitude et à la sécurité des données d'Eurodac. Toute personne ou tout État membre qui a subi un dommage en raison du non-respect de dispositions d'Eurodac a le droit d'obtenir réparation de l'État membre qui est responsable du dommage subi.

Le règlement (UE) n° 603/2013 prévoit l'accès aux données d'Eurodac par les autorités désignées des États membres et par Europol à des fins répressives. Conformément au règlement, les autorités désignées ne peuvent présenter de demande électronique motivée de comparaison de données dactyloscopiques avec les données conservées dans le système central que si la comparaison dans les bases de données ci-après n'a pas permis de déterminer l'identité de la personne concernée:

– les bases de données dactyloscopiques nationales;

[58] Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, JO L 286 du 1.11.2011, p. 1.

– les systèmes de reconnaissance automatisée d'empreintes digitales (AFIS) de tous les autres États membres au titre de la décision 2008/615/JAI ("décisions Prüm"), si les comparaisons sont disponibles techniquement, à moins qu'il n'existe des motifs raisonnables de croire qu'une comparaison avec ces systèmes ne permettraient pas de déterminer l'identité de la personne concernée. De tels motifs raisonnables figurent dans la demande électronique motivée de comparaison avec les données d'Eurodac adressée par l'autorité désignée à l'autorité de vérification;

– le Système d'information sur les visas (VIS), pour autant que les conditions d'une telle comparaison prévues dans la décision 2008/633/JAI soient réunies.

Les conditions cumulées suivantes doivent aussi être remplies:

a) La comparaison est nécessaire aux fins de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes en la matière, en ce sens qu'il existe un intérêt supérieur de sécurité publique qui rend la consultation de la base de données proportionnée.

b) La comparaison est nécessaire dans un cas précis (c'est-à-dire des comparaisons systématiques ne peuvent être effectuées).

c) Il existe des motifs raisonnables de penser que la comparaison contribuera de manière significative à la prévention ou à la détection de l'une des infractions pénales en question et aux enquêtes en la matière. De tels motifs raisonnables existent en particulier lorsqu'il y a des motifs de soupçonner que le suspect, l'auteur ou la victime d'une infraction terroriste ou d'une autre infraction pénale grave relève d'une catégorie couverte par le règlement (UE) n° 603/2013.

2.8. SID – Système d'information douanier[59]

Le système d'information douanier complète la Convention Naples II[60]. Le système vise à renforcer l'administration douanière des États membres grâce à un échange d'informations rapide, en vue de prévenir les infractions graves aux lois nationales et communautaires, d'enquêter sur elles et de les poursuivre. Le SID met également en place un fichier d'identification des dossiers (FIDE) afin d'assister les enquêtes douanières.

Le SID, géré par la Commission, est un système d'information centralisé accessible à partir de terminaux dans chacun des États membres et à la Commission, Europol et Eurojust. Les autorités douanières, fiscales, agricoles, de santé publique et policières nationales, Europol et Eurojust peuvent accéder aux données du SID. Seules les autorités désignées par les États membres[61] et la Commission ont directement accès aux données contenues dans le SID. Afin de renforcer leur complémentarité, Europol et Eurojust disposent d'un accès en lecture seule au SID et au FIDE.

Le SID comprend les données à caractère personnel se rapportant à des marchandises, moyens de transports, entreprises, personnes et retenues, saisies ou confiscations d'articles et d'argent liquide. Les données à caractère personnel ne peuvent être copiées du SID dans d'autres systèmes de traitement des données qu'à des fins d'analyses opérationnelles ou de gestion des risques, et seuls les analystes désignés par les États membres peuvent y accéder.

Le FIDE permet aux autorités nationales chargées de mener des enquêtes en matière douanière, lorsqu'elles ouvrent un dossier d'enquête, d'identifier les autres autorités qui auraient pu enquêter sur une personne ou une entreprise donnée.

---

59 Décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes, JO L 323 du 10.12.2009, p. 20.

60 Convention établie sur la base de l'article K.3 du traité sur l'Union européenne, relative à l'assistance mutuelle et à la coopération entre les administrations douanières, JO C 24 du 23.1.1998, p. 2.

61 Mise en œuvre de l'article 7, paragraphe 2, et de l'article 8, paragraphe 3, de la décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes - listes actualisées des autorités compétentes, doc. 13394/11 ENFOCUSTOM 85.

2.9. Faux documents et documents authentiques en ligne - FADO[62]

Un système informatisé d'archivage comportant des images de documents faux et authentiques et fondé sur la technologie internet permet un échange d'informations rapide et sûr entre le Secrétariat général du Conseil de l'Union européenne et les contrôleurs de documents dans tous les États membres, ainsi qu'en Islande, en Norvège et en Suisse. Le système permet de procéder à une comparaison à l'écran entre le document original et un document faux ou falsifié. Il contient surtout des documents des États membres, ainsi que des documents des pays tiers en provenance desquels il y a un flux d'immigration constant vers les États membres. La base de données créée avec FADO inclut les données suivantes:

- des images de documents authentiques;
- des informations sur les techniques de sécurité (éléments de sécurité);
- des images de documents contrefaits et falsifiés typiques;
- des informations sur les techniques de falsification; et
- des statistiques relatives aux documents faux ou falsifiés détectés ainsi qu'à l'usurpation d'identité.

Le système utilise des lignes spéciales pour la transmission des données entre le Secrétariat général du Conseil et les unités centrales des États membres. À l'intérieur de chaque État membre, le système est consulté par l'intermédiaire d'une connexion internet sécurisé à partir d'une unité centrale. Un État membre peut utiliser le système pour un usage interne sur son territoire, c'est-à-dire en reliant entre eux plusieurs terminaux installés à ses différents postes de contrôle frontaliers ou auprès d'autres autorités compétentes. Toutefois, il n'y a pas de liaison directe entre un poste de travail, autre qu'une unité centrale nationale, et le point central situé au sein du Secrétariat général.

FADO est actuellement disponible en 22 langues officielles de l'Union européenne. La saisie des documents est effectuée par des experts en documents dans l'une des langues prévues et des descriptions normalisées sont traduites automatiquement. En conséquence, les documents sont immédiatement disponibles dans toutes les langues couvertes. Des commentaires supplémentaires en texte libre sont traduits ultérieurement par les traducteurs spécialisés au sein du Secrétariat général du Conseil.

---

62 Action commune 98/700/JAI du 3 décembre 1998 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la création d'un système européen d'archivage d'images (FADO), JO L 333 du 9.12.1998, p. 4.

2.10. Registre public en ligne des documents authentiques d'identité et de voyage - PRADO

Alors que l'accès à FADO est limité aux contrôleurs de documents et à une utilisation par les pouvoirs publics, le Registre public en ligne des documents authentiques d'identité et de voyage (PRADO) du Conseil de l'Union européenne contient un sous-ensemble de données FADO qui sont mises à la disposition du public. Le site web[63] est publié dans les langues officielles de l'UE par le Secrétariat général du Conseil de l'Union européenne, pour des raisons de transparence, et il fournit un service important à de nombreux utilisateurs en Europe, en particulier aux organisations non gouvernementales ayant le besoin ou l'obligation légale de procéder à des contrôles d'identité.

Le site web contient des descriptions techniques, y compris des informations sur les éléments de sécurité, de documents d'identité et de voyage authentiques. Les informations sont choisies et mises à disposition par des experts en documents dans les États membres, l'Islande, la Norvège et la Suisse.

Dans PRADO, les utilisateurs peuvent aussi trouver des liens vers des sites web contenant des informations sur les numéros de document invalides fournies par certains États membres, ainsi que par des pays tiers, et d'autres informations utiles relatives à la vérification et à la fraude en matière d'identité et de documents.

2.11. Système d'entrée/de sortie (EES)

Le système d'entrée/de sortie[64] (EES) vise principalement à améliorer la gestion des frontières extérieures de l'Union[65]. Il enregistre de manière électronique l'heure et le lieu d'entrée et de sortie de certains ressortissants de pays tiers qui sont admis pour un court séjour sur le territoire des États membres et calcule la durée de leur séjour autorisé.

En outre, l'EES peut être consulté, uniquement dans les conditions prévues dans le règlement, par les services répressifs nationaux aux fins de la prévention et de la détection des infractions terroristes et d'autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière.

---

63 http://www.prado.consilium.europa.eu/

64 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.

65 La Commission fixera la date à laquelle l'EES doit être mis en service, une fois que les conditions énoncées à l'article 66 du règlement (UE) 2017/2226 sont remplies.

Le règlement établit des règles strictes d'accès à l'EES. Il fixe aussi le droit des personnes concernées à accéder aux données, à les faire rectifier, compléter, et effacer, ainsi que leur droit à un recours, en particulier le droit à un recours juridictionnel, et prévoit le contrôle des opérations de traitement par des autorités publiques indépendantes. Le règlement respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne.

L'EES est composé des éléments suivants:

- un système central (le système central de l'EES), qui gère une base de données centrale informatisée comprenant des données biométriques (données dactyloscopiques et images faciales) et alphanumériques,
- une interface uniforme nationale dans chaque État membre,
- une infrastructure de communication sécurisée et cryptée, qui permet de connecter le système central de l'EES à l'interface uniforme nationale,
- un canal de communication sécurisé, qui relie le système central de l'EES au système central d'information sur les visas (système central du VIS) à des fins de consultation.

Le règlement détermine quelles autorités nationales sont habilitées à avoir accès à l'EES pour introduire, modifier, effacer ou consulter des données pour les besoins propres de l'EES et dans la mesure nécessaire à l'exécution de leurs tâches. Tout traitement des données de l'EES devrait être proportionné aux objectifs poursuivis et nécessaire à l'exécution des tâches des autorités compétentes.

Les conditions d'accès des services répressifs nationaux à l'EES permettent à ces derniers de s'attaquer aux cas de suspects utilisant plusieurs identités. Malgré son incidence sur la vie privée des voyageurs, l'utilisation spécifique des données biométriques stockées dans l'EES est justifiée pour identifier les voyageurs qui ne sont pas en possession de documents de voyage ou d'un autre moyen d'identification. Par ailleurs, ces données peuvent également servir à rassembler des preuves en surveillant les déplacements d'une personne soupçonnée d'avoir commis une infraction grave ou les déplacements d'une victime d'une infraction grave.

L'accès à l'EES à des fins répressives constitue une atteinte aux droits fondamentaux que sont le respect de la vie privée des personnes et la protection des données à caractère personnel des personnes dont les données sont traitées dans l'EES. Un tel traitement est régi par les dispositions de la directive (UE) 2016/680 (directive "police" relative à la protection des données)[66].

Aux fins de l'exécution de leurs tâches, les services répressifs nationaux peuvent comparer une trace dactyloscopique trouvée sur une scène de crime ("empreinte latente") avec les données dactyloscopiques qui sont stockées dans l'EES, lorsqu'il existe des motifs raisonnables de croire que l'auteur ou la victime est enregistré dans l'EES. En revanche, l'accès à l'EES à des fins répressives en vue d'identifier un suspect inconnu ou l'auteur inconnu d'une infraction terroriste ou d'une autre infraction pénale grave, ou des victimes inconnues de telles infractions, est subordonné à la condition que les consultations des bases de données nationales aient été effectuées et que les recherches sur la base des empreintes digitales dans le cadre de la décision 2008/615/JAI du Conseil[67] (décision Prüm) aient été effectuées intégralement, ou que ces recherches n'aient pas été effectuées intégralement dans les deux jours suivant leur lancement.

À l'instar des procédures et des conditions qui régissent l'accès des services répressifs nationaux, Europol a également accès aux données de l'EES, dans le cadre de ses missions et sous réserve des conditions et des limitations prévues dans le règlement. Europol traite les informations obtenues à la suite de la consultation des données de l'EES, sous réserve de l'autorisation de l'État membre d'origine. Cette autorisation est obtenue par l'intermédiaire de l'unité nationale Europol de cet État membre. Le Contrôleur européen de la protection des données devrait contrôler le traitement des données par Europol et garantir le plein respect des règles applicables en matière de protection des données.

---

66 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2019 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

67 Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210 du 6.8.2008, p. 1.

2.12. Système européen d'information et d'autorisation concernant les voyages (ETIAS)[68]

L'échange d'informations aux fins de la gestion des frontières, du contrôle de l'application de la loi et de la lutte contre le terrorisme sera soutenu par l'ETIAS[69]. Ce système a pour objectif de déterminer si les ressortissants de pays tiers exemptés de l'obligation de visa remplissent les conditions applicables, préalablement à leur voyage vers l'espace Schengen et avant leur arrivée aux points de passage des frontières extérieures. L'ETIAS fournit une autorisation de voyage, qui est par nature différente d'un visa mais constitue une condition d'entrée et de séjour, et qui indique que le demandeur ne présente pas un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé. Les autorisations de voyage délivrées devraient être annulées ou révoquées dès qu'il s'avère que les conditions de délivrance requises n'étaient pas ou ne sont plus remplies.

L'ETIAS est composé:

- d'un système d'information à grande échelle, le système d'information ETIAS, dont la conception, le développement et la gestion technique sont assurés par l'eu-LISA;
- de l'unité centrale ETIAS, qui fait partie de l'Agence européenne de garde-frontières et de garde-côtes;
- des unités nationales ETIAS, qui sont chargées d'examiner les demandes et de décider de délivrer, de refuser, d'annuler ou de révoquer les autorisations de voyage. À cette fin, les unités nationales devraient coopérer entre elles ainsi qu'avec Europol aux fins de l'évaluation des demandes.

---

68 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. Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), JO L 236 du 19.9.2018, p. 72.

69 La Commission fixera la date à laquelle l'ETIAS doit être mis en service, une fois que les conditions énoncées à l'article 88 du règlement (UE) 2018/1240 sont remplies.

Les données à caractère personnel fournies par le demandeur sont traitées par l'ETIAS aux seules fins d'évaluer si l'entrée du demandeur dans l'Union est susceptible de représenter un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé dans l'Union. Aux fins de l'évaluation des risques, les données à caractère personnel fournies devraient être comparées aux données contenues dans les relevés, les dossiers ou les signalements enregistrés dans un système d'information ou une base de données de l'UE (le système central ETIAS, le SIS, le système d'information sur les visas (VIS), le système d'entrée/de sortie (EES) ou Eurodac), dans les données Europol ou dans les bases de données d'Interpol (la base de données d'Interpol sur les documents de voyage volés ou perdus (SLTD) ou la base de données d'Interpol sur les documents de voyage associés aux notices (TDAWN)). Les données à caractère personnel devraient également être comparées à la liste de surveillance ETIAS et à des indicateurs de risques spécifiques.

La comparaison est effectuée selon des procédés automatisés. En cas de réponse positive ("hit"), c'est-à-dire lorsqu'il y a correspondance entre des données de la demande et les indicateurs de risques spécifiques ou les données à caractère personnel contenues dans un relevé, un dossier ou un signalement figurant dans les systèmes d'information susmentionnés ou dans la liste de surveillance, la demande devrait être traitée manuellement par l'unité nationale de l'État membre responsable. Cette évaluation devrait aboutir à la décision de délivrer ou non l'autorisation de voyage.

La réalisation des objectifs globaux de l'ETIAS nécessite de traiter des volumes importants de données à caractère personnel. Le règlement respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne. Des garanties appropriées visent par conséquent à limiter l'ingérence vis-à-vis du droit à la protection de la vie privée et du droit à la protection des données à caractère personnel à ce qui est nécessaire et proportionné dans une société démocratique. Pour la même raison, les critères utilisés pour définir les indicateurs de risques spécifiques ne devraient en aucun cas être fondés sur des données à caractère personnel sensibles[70].

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

L'accès aux données à caractère personnel figurant dans l'ETIAS devrait être limité au personnel strictement autorisé et ne devrait en aucun cas être utilisé pour prendre des décisions fondées sur l'une ou l'autre forme de discrimination. En ce qui concerne les services répressifs, le traitement de données à caractère personnel stockées dans le système central ETIAS ne devrait avoir lieu que dans des cas spécifiques et pour autant que cela soit nécessaire aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux fins des enquêtes en la matière. Les autorités désignées et Europol ne devraient demander l'accès à l'ETIAS que lorsqu'elles ont des motifs raisonnables de penser que cet accès leur permettra d'obtenir des informations qui les aideront à prévenir ou à détecter une infraction terroriste ou une autre infraction pénale grave, ou à enquêter en la matière.

2.13. Tableau synthétique des systèmes d'information utilisés pour l'échange d'information dans l'UE

Systèmes informatiques et bases de données	Base juridique	Finalités de l'utilisation	Personnes concernées	Partage des données
Système d'information Schengen de deuxième génération - **SIS II**	Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) JO L 205 du 7.8.2007, p. 63	• Sécurité intérieure • Contrôle aux frontières • Coopération judiciaire • Enquêtes criminelles	• Citoyens de l'UE • Ressortissants de pays tiers	• VIS • Europol • Eurojust • Interpol
	Règlement (CE) n° 1987/2006 du Parlement Européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) JO L 381 du 23.12.2006, p. 4	• Non-admission ou interdiction de séjour • Politiques en matière d'asile, d'immigration et de retour	• Ressortissants de pays tiers ne bénéficiant pas de droits en matière de libre circulation équivalents à ceux des citoyens de l'Union	
	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	• Non-admission ou interdiction de séjour • Contrôle aux frontières • Enquêtes criminelles	• Ressortissants de pays tiers	• Europol • Agence européenne de garde-frontières et de garde-côtes (Frontex).

	Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier JO L 312 du 7.12.2018, p. 1	• Politiques en matière de migration et de retour	• Ressortissants de pays tiers	• Europol • Agence européenne de garde-frontières et de garde-côtes (Frontex).
	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	• Sécurité intérieure • Contrôle aux frontières • Coopération judiciaire • Enquêtes criminelles		
Europol **SIE**	Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), articles 11 à 13 JO L 121 du 15.5.2009, p. 37	• Infractions graves • Immigration • Sécurité intérieure • Lutte contre le terrorisme	• Citoyens de l'UE • Ressortissants de pays tiers	• SIS II
Interpol **I-24/7**	Constitution d'Interpol		• Citoyens de l'UE • Ressortissants de pays tiers	• SIS II • Europol • VIS

Interpol **Documents de voyage perdus ou volés**	Position commune 2005/69/JAI du Conseil relative à l'échange de certaines données avec Interpol JO L 27 du 29.1.2005, p. 61	• Criminalité internationale et organisée • Sécurité intérieure	• Citoyens de l'UE • Ressortissants de pays tiers	
ECRIS	Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil JO L 151 du 7.6.2019, p. 143	• Procédures pénales	• Citoyens de l'UE • Ressortissants de pays tiers	
ECRIS-TCN	Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 JO L 135 du 22.5.2019, p. 1 Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil JO L 151 du 7.6.2019, p. 143	• Procédures pénales	• Ressortissants de pays tiers	• Europol • Eurojust • Parquet européen

VIS	Décision 2004/512/CE du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS) JO L 213 du 15.6.2004, p. 5 Décision 2008/633/JAI du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière JO L 218 du 13.8.2008, p. 129 Décision 2013/392/UE du Conseil fixant la date de prise d'effet de la décision 2008/633/JAI concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière JO L 198 du 23.7.2013, p. 45	• Infractions graves • Sécurité intérieure • Lutte contre le terrorisme	• Ressortissants de pays tiers	• SIS II • Europol • Interpol

Eurodac	Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte) JO L 180 du 29.6.2013, p. 1 Règlement (UE) n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride JO L 180 du 29.6.2013, p. 31	• Immigration • Infractions graves • Sécurité intérieure • Lutte contre le terrorisme	• Ressortissants de pays tiers	• Europol

Dossiers passagers **(PNR)**	Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière JO L 119 du 4.5.2016, p. 132	• Infractions graves • Sécurité intérieure • Lutte contre le terrorisme	• Citoyens de l'UE • Ressortissants de pays tiers	• Europol
Informations préalables sur les passagers (données API)	Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers JO L 261 du 6.8.2004, p. 24	• Contrôle aux frontières • Immigration	• Ressortissants de pays tiers	
ETIAS	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[71] JO L 236 du 19.9.2018, p. 1 Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) JO L 236 du 19.9.2018, p. 72	• Contrôle aux frontières • Immigration • Infractions graves • Sécurité intérieure • Lutte contre le terrorisme	• Ressortissants de pays tiers	• SIS • VIS • EES • Eurodac • Europol • Interpol • Liste de surveillance ETIAS

[71] La Commission fixera la date à laquelle l'ETIAS doit être mis en service, une fois que les conditions énoncées à l'article 88 du règlement sont remplies.

EES	Règlement (UE) 2017/2225 du Parlement européen et du Conseil du 30 novembre 2017 modifiant le règlement (UE) 2016/399 en ce qui concerne l'utilisation du système d'entrée/de sortie JO L 327 du 9.12.2017, p. 1 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[72]. JO L 327 du 9.12.2017, p. 20	• Gestion des frontières • Infractions graves • Lutte contre le terrorisme	• Ressortissants de pays tiers	• VIS • Europol • Décision Prüm
SIC	Décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes JO L 323 du 10.12.2009, p. 20	• Lutte contre les trafics illicites	• Citoyens européens • Ressortissants de pays tiers	• Europol

[72] La Commission fixera la date à laquelle l'EES doit être mis en service, une fois que les conditions énoncées à l'article 66 du règlement sont remplies.

FADO	Action commune (98/700/JAI) du 3 décembre 1998 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la création d'un système européen d'archivage d'images (FADO) JO L 333 du 9.12.1998, p. 4	• Lutte contre les faux documents • Politique d'immigration • Coopération policière	• Citoyens européens • Ressortissants de pays tiers	

3. LEGISLATION - CONTEXTE JURIDIQUE, REGLES ET ORIENTATIONS RELATIFS AUX PRINCIPAUX MODES ET SYSTEMES DE COMMUNICATION

3.1. Directive sur la protection des données[73]

La directive (UE) 2016/680, qui abroge la décision-cadre 2008/977/JAI du Conseil[74], fixe les règles spécifiques relatives:

- à la protection des personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, à l'égard du traitement, à l'aide de procédés automatisés ou d'une autre manière, de données à caractère personnel par la police ou d'autres autorités répressives dans le cadre de leurs activités, et

- à l'échange de données à caractère personnel au sein de l'Union 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.

Elle vise à assurer le même niveau de protection pour les personnes physiques par l'instauration de de droits opposables dans l'ensemble de l'Union et à éviter des pratiques divergentes qui entravent les échanges de données à caractère personnel entre les autorités compétentes.

Les États membres doivent transposer cette directive au plus tard le 6 mai 2018. Toutefois, dans les cas où cela nécessite un effort disproportionné, ils peuvent prévoir, à titre exceptionnel, de mettre en œuvre, d'ici le 6 mai 2023, les dispositions pertinentes en matière de suivi des opérations effectuées dans des systèmes de traitement automatisé mis en place avant le 6 mai 2016.

---

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

74 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 60. La décision-cadre est abrogée avec effet au 6 mai 2018.

Le terme "autorités compétentes" couvre les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. Les activités des autorités répressives sont axées principalement sur la prévention et la détection des infractions pénales et les enquêtes et les poursuites en la matière. Ces activités peuvent également comprendre les activités de police lors de manifestations, de grands événements sportifs et d'émeutes. Parmi ces activités figure également le maintien de l'ordre public lorsque cette mission leur est confiée lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale.

Le traitement des données à caractère personnel à des fins en dehors du champ d'application des activités susmentionnées et que les États membres peuvent confier en plus aux autorités répressives est régi par le règlement (UE) 2016/679[75], tout comme le traitement des données à caractère personnel, pour autant que celui-ci relève du champ d'application du droit de l'Union. De plus, la directive (UE) 2016/680 ne couvre pas le traitement des données à caractère personnel effectué dans le cadre des activités relatives à la sécurité nationale, des activités des agences ou des services responsables des questions de sécurité nationale ou du traitement de données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune[76].

Aux fins de la directive sur la protection des données, on entend par:

- **"données à caractère personnel"**, toute information se rapportant à une personne physique (ci-après dénommée "personne concernée") identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

  Les États membres prévoient que les autorités compétentes traitant des données à caractère personnel établissent, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que a) les suspects, b) les personnes condamnées, c) les victimes et d) les tiers à une infraction pénale, notamment les témoins;

---

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

[76] Titre V, chapitre 2, du traité sur l'Union européenne (TUE).

- **"traitement"**, toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Les données à caractère personnel doivent être traitées de manière licite et loyale, et uniquement aux fins spécifiques fixées par la loi. Pour être licite, ce traitement devrait être nécessaire à l'exécution d'une mission par une autorité compétente aux fins répressives susmentionnées. Le principe de traitement loyal en matière de protection des données est une notion distincte du droit à accéder à un tribunal impartial défini à l'article 47 de la Charte et à l'article 6 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales. Les données à caractère personnel doivent être adéquates et pertinentes au regard des finalités pour lesquelles elles sont traitées.

Le traitement des données à caractère personnel particulièrement sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et seulement à des conditions bien définies et restrictives.

L'institution d'autorités de contrôle nationales qui sont en mesure d'exercer leurs fonctions en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement de leurs données. Il y a lieu que les autorités de contrôle surveillent l'application des dispositions adoptées en vertu de la directive et contribuent à ce que son application soit cohérente dans l'ensemble de l'Union. La protection des droits et des libertés des personnes concernées, de même que la responsabilité des autorités nationales compétentes et des sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par celles-ci, exige une répartition claire des responsabilités.

Le franchissement des frontières par les données à caractère personnel peut mettre en péril la capacité des personnes physiques à se protéger sur le plan légal contre l'utilisation ou la divulgation illicite de ces données. De même, les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontière peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours et par l'hétérogénéité des régimes juridiques. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, afin qu'elles puissent échanger des informations avec leurs homologues étrangers.

3.2. Décision-cadre suédoise[77]

Dans le cadre du développement de l'acquis de Schengen, la décision-cadre 2006/960/JAI du Conseil ("décision-cadre suédoise") fixe, en particulier, les règles relatives aux délais et aux formulaires types pour l'échange transfrontière d'informations[78], en réponse à une demande préalable ou spontanément, entre les services répressifs compétents désignés des États membres aux fins:

- de prévenir et de détecter des infractions ou des activités criminelles, ainsi que d'enquêter sur celles-ci, lorsqu'elles correspondent ou sont équivalentes à celles visées par le mandat d'arrêt européen[79], ou
- de prévenir un danger immédiat et sérieux pour la sécurité publique.

Les autorités désignées sont tenues de répondre dans un délai maximum de huit heures dans les cas urgents, dès lors que les informations ou renseignements demandés sont directement accessibles aux services répressifs. Les informations peuvent ne pas être fournies dans les cas suivants:

- la sécurité nationale est en jeu,
- des enquêtes en cours pourraient être mises en péril,

---

77 Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, JO L 386 du 29.12.2006, p. 89, corrigée par le rectificatif publié au JO L 75 du 15.7.2007, p. 26.

78 Voir figure 1 infra.

79 Doc. 8216/2/08 REV 2, version finale du manuel européen concernant l'émission d'un mandat d'arrêt européen. L'article 2 de la décision-cadre 2002/584/JAI du Conseil relatif au mandat d'arrêt européen (MAE) définit le champ d'application du MAE.

- la demande concerne une infraction punissable d'une peine d'emprisonnement d'un an ou moins en vertu du droit de l'État membre requis,

- l'autorité judiciaire compétente bloque l'accès aux informations.

L'expression "informations et/ou renseignements" couvre les deux catégories suivantes:

– tout type d'informations ou de données détenues par des services répressifs,

– tout type d'informations ou de données détenues par des autorités publiques ou par des entités privées et qui sont accessibles aux services répressifs sans que des mesures coercitives ne soient prises.

Le contenu de ces catégories dépend de la législation nationale. Les types d'informations rendus disponibles par chaque État membre sont définis dans les fiches nationales jointes au présent manuel.

Les données doivent être échangées avec Europol dans la mesure où les informations ou renseignements échangés portent sur une infraction ou une activité délictueuse qui relève du mandat d'Europol. Informations et renseignements seront traités conformément aux codes de traitement pertinents d'Europol. SIENA (l'application de réseau d'échange sécurisé d'informations d'Europol) est utilisée pour faciliter l'échange d'informations conformément à la "décision-cadre suédoise".

Les États membres veillent à ce que les conditions de l'échange transfrontière d'informations ne soient pas plus strictes que celles qui s'appliqueraient dans une affaire interne. En particulier, les services répressifs compétents ne sont pas obligés de conditionner l'échange transfrontière d'informations à l'obtention d'un accord ou d'une autorisation judiciaire si les informations souhaitées sont disponibles au niveau national sans nécessiter un tel accord ou une telle autorisation. Si, toutefois, une autorisation judiciaire est requise, l'autorité judiciaire est tenue d'appliquer à sa décision dans une affaire transfrontière les mêmes règles que pour une affaire purement interne. Les informations pour lesquelles une autorisation judiciaire est nécessaire sont indiquées dans les fiches nationales.

Étant donné que le formulaire type de demande a été jugé trop complexe par les praticiens, un formulaire facultatif de demande d'information et de renseignements[80] a été élaboré. Lorsqu'il n'est pas possible d'utiliser ce formulaire simplifié, la préférence est donnée à l'utilisation d'un autre formulaire ou au recours à du texte libre non structuré.

---

80 Voir figure 2 infra.

Toutefois, ces demandes doivent satisfaire, dans tous les cas, aux exigences de l'article 5 de la décision-cadre suédoise, et contenir au moins les éléments obligatoires suivants:

- Informations administratives: État membre requérant, service requérant, date, numéro(s) de référence, État(s) membre(s) requis
- Traitement d'urgence demandé ou non et, si tel est le cas, les motifs de la demande de traitement d'urgence
- Description des informations ou renseignements demandés
- Identité (dans la mesure où elle est connue) de la ou des personnes ou du ou des objets faisant l'objet principal de l'enquête pénale ou de l'opération de renseignement en matière pénale justifiant la demande d'informations ou de renseignements (par exemple, description de l'infraction ou des infractions, circonstances dans lesquelles l'infraction ou les infractions ont été commises, etc.)
- Fins auxquelles les informations et les renseignements sont sollicités
- Lien entre ces fins et la personne qui fait l'objet de ces informations ou de ces renseignements
- Raisons permettant de penser que les informations ou les renseignements se trouvent dans l'État membre requis
- Restrictions éventuelles concernant l'utilisation des informations figurant dans la demande ("codes de traitement")

L'État membre requérant peut choisir l'un des canaux existants en matière de communication internationale en matière répressive (SIRENE, EUROPOL, INTERPOL, points de contacts bilatéraux). L'État membre qui apporte la réponse recourt normalement au même canal que celui qui a été utilisé pour introduire la demande. Toutefois, si, pour des raisons légitimes, l'État membre requis répond par un autre canal, l'autorité requérante en est informée. La langue utilisée pour la demande et la fourniture d'informations est celle prévue pour le canal retenu.

Un aperçu des **accords bilatéraux ou autres maintenus en vigueur**, est annexé au présent manuel.

Figure 1

ANNEXE A

ÉCHANGE D'INFORMATIONS AU TITRE DE LA DÉCISION-CADRE 2006/960/JAI DU CONSEIL FORMULAIRE À UTILISER PAR L'ÉTAT MEMBRE REQUIS EN CAS DE TRANSMISSION D'INFORMATIONS OU DE RETARD/REFUS DE TRANSMISSION DES INFORMATIONS

Le présent formulaire doit être utilisé pour transmettre les informations et/ou les renseignements requis, informer le service requérant de l'impossibilité de respecter le délai normal, de la nécessité de soumettre la demande à l'autorisation d'une autorité judiciaire ou du refus de transmettre les informations.

Le présent formulaire peut être utilisé plusieurs fois au cours de la procédure (par exemple, si la demande doit d'abord être soumise à une autorité judiciaire et qu'il s'avère par la suite que l'exécution de la demande doit être refusée).

Autorité requise (nom, adresse, n° de téléphone, n° de télécopie, adresse électronique, État membre)	
Coordonnées de l'agent chargé du suivi (facultatif)	
Numéro de référence de la présente réponse	
Date et numéro de référence de la réponse précédente	
Réponse à l'autorité requérante suivante	
Date et heure de la demande	
Numéro de référence de la demande	

Délai normal prévu à l'article 4 de la décision-cadre 2006/960/JAI	
L'infraction relève de l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI et les informations ou les renseignements demandés figurent dans une base de données à laquelle un service répressif peut avoir directement accès dans l'État membre requis.	Traitement d'urgence demandé → ❑ 8 heures
	Traitement d'urgence non demandé → ❑ 1 semaine
Autres cas	→ ❑14 jours

Informations transmises en application de la décision-cadre : 2006/960JAI*: informations et renseignements fournis
1. L'utilisation des informations ou des renseignements fournis ❑ n'est autorisée qu'aux fins pour lesquelles ceux-ci ont été communiqués ou pour prévenir un danger immédiat et sérieux pour la sécurité publique; ❑ est également autorisée à d'autres fins, sous réserve des conditions suivantes (facultatif):.....;
2. Fiabilité de la source ❑ fiable ❑ généralement fiable ❑ pas fiable ❑ ne peut être évaluée
3. Fiabilité des informations ou renseignements ❑ sûrs ❑ attestés par la source ❑ Ouï-dire - confirmés ❑ Ouï-dire - non confirmés

4. Les résultats de l'enquête pénale ou de l'opération de renseignement en matière pénale qui a donné lieu à l'échange d'informations et de renseignements doivent être communiqués à l'autorité qui a transmis ces informations ou renseignements

❑ non
❑ oui

5. En cas d'échange spontané, raisons qui donnent lieu de croire que les informations ou renseignements pourraient contribuer au dépistage et à la prévention des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, ou à une enquête à leur sujet:

RETARD - Il n'est pas possible de répondre dans le délai applicable prévu à l'article 4 de la décision-cadre 2006/960/JAI

Les informations ou les renseignements ne peuvent être communiqués dans le délai indiqué pour les raisons suivantes:

Ils devraient pouvoir être transmis dans:

❑ 1 jour ❑ 2 jours ❑ 3 jours
❑ ... semaines
❑ 1 mois

❑ L'autorisation a été demandée à une autorité judiciaire.
La durée prévue de la procédure d'octroi ou de refus de l'autorisation est de ... semaines.

REFUS - Les informations ou les renseignements:
❑ n'ont pu être communiqués et demandés au niveau national; ou
❑ ne peuvent être communiqués, pour une ou plusieurs des raisons suivantes:

A - Raison liée au contrôle juridictionnel qui empêche la transmission ou nécessite le recours à l'entraide judiciaire

❑ L'autorité judiciaire compétente n'a pas autorisé l'accès aux informations ou aux renseignements, ni leur échange.

❑ Les informations ou les renseignements demandés ont été obtenus précédemment au moyen de mesures coercitives et leur transmission n'est pas autorisée par le droit national.

❑ Les informations ou les renseignements ne sont pas détenus

- par des services répressifs; ou
- par des autorités publiques ou par des entités privées d'une façon qui permette aux services répressifs d'y accéder sans prendre de mesures coercitives.

❑ B - La communication des informations ou des renseignements demandés porterait atteinte aux intérêts vitaux de l'État membre requis en matière de sécurité nationale ou nuirait au bon déroulement d'une enquête ou d'une opération de renseignement en matière pénale ou à la sécurité des personnes ou les informations ou les renseignements demandés sont clairement disproportionnés ou sans objet au regard des finalités pour lesquelles ils ont été demandés.

Si vous cochez la case A ou B, veuillez fournir, les informations complémentaires que vous jugez utiles ou indiquer le motif du refus (facultatif):

❑ D - L'autorité requise décide de refuser l'exécution car la demande concerne, dans le droit de l'État membre requis, l'infraction suivante (préciser la nature et la qualification juridique de l'infraction)..... qui est punissable d'une peine d'emprisonnement d'un an ou moins.

❑ E - Les informations ou les renseignements demandés ne sont pas disponibles.

❑ F - Les informations ou les renseignements demandés ont été obtenus auprès d'un autre État membre ou d'un pays tiers et sont soumis au principe de spécialité, et cet État membre ou pays tiers n'a pas donné son accord pour que ces informations ou ces renseignements soient communiqués.

ANNEXE B

ÉCHANGE D'INFORMATIONS AU TITRE DE LA DÉCISION-CADRE 2006/960/JAI DU CONSEIL FORMULAIRE DE DEMANDE D'INFORMATIONS ET DE RENSEIGNEMENTS À UTILISER PAR L'ÉTAT MEMBRE REQUÉRANT

Le présent formulaire doit être utilisé pour demander des informations et des renseignements au titre de la décision-cadre 2006/960/JAI

I - Informations administratives

Service requérant (nom, adresse, n° de téléphone, n° de télécopie, adresse électronique, État membre)	
Coordonnées de l'agent chargé du suivi (facultatif)	
À l'État membre suivant	
Date et heure de la présente demande	
Numéro de référence de la présente demande	

Demandes précédentes				
❑ La présente demande est la première dans cette affaire				
❑ La présente demande fait suite à d'autres demandes concernant la même affaire				
Demande(s) précédente(s)			Réponse(s)	
	Date	Numéro de référence (pour l'État requérant)	Date	Numéro de référence (pour l'État requis)
1.				
2.				
3.				
4.				

Si la présente demande est adressée à plusieurs autorités de l'État membre requis, veuillez préciser par quels canaux	
❑ Officier de liaison UNE/Europol	❑ Pour information ❑ Pour exécution
❑ BCN Interpol	❑ Pour information ❑ Pour exécution
❑ SIRENE	❑ Pour information ❑ Pour exécution
❑ Officier de liaison	❑ Pour information ❑ Pour exécution
❑ Autre (veuillez préciser)	❑ Pour information ❑ Pour exécution
Si la même demande est adressée à d'autres États membres, veuillez préciser ces États membres, ainsi que les canaux utilisés (facultatif)	

II — Délais

Rappel: délais prévus à l'article 4 de la décision-cadre 2006/960/JAI

A — L'infraction relève de l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI

et

les informations ou les renseignements demandés figurent dans une base de données à laquelle un service répressif peut avoir directement accès:

→ La demande est urgente → Délai: huit heures, avec possibilité de report

→ La demande n'est pas urgente → Délai: une semaine(...)

B — Autres cas: délai: quatorze jours (...)

❑ **Un traitement d'urgence EST demandé.**
❑ **Un traitement d'urgence N'EST PAS demandé.**
Motifs du traitement d'urgence (par exemple: les suspects sont maintenus en détention, l'affaire doit être portée en justice avant une date déterminée):
Informations ou renseignements demandés

Type de criminalité ou d'activité(s) criminelle(s) faisant l'objet de l'enquête
Description des circonstances de la commission de l'infraction (des infractions), y compris le moment, le lieu et le degré de participation à l'infraction (aux infractions) de la personne au sujet de laquelle les informations ou les renseignements sont demandés:

Nature de l'infraction (des infractions)

A – Application de l'article 4, paragraphes 1 et 3, de la décision-cadre 2006/960/JAI

❑ A.1. L'infraction est punissable d'une peine d'emprisonnement maximale de trois ans au moins dans l'État membre requérant.
ET
A.2. L'infraction est l'une (ou plusieurs) des infractions suivantes:

- ❑ Participation à une organisation criminelle
- ❑ Terrorisme
- ❑ Traite des êtres humains
- ❑ Exploitation sexuelle des enfants et pédopornographie
- ❑ Trafic de stupéfiants et de substances psychotropes
- ❑ Trafic d'armes, de munitions et d'explosifs
- ❑ Corruption
- ❑ Fraude, y compris la fraude portant atteinte aux intérêts financiers des Communautés européennes au sens de la convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes
- ❑ Vol organisé ou à main armée
- ❑ Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art
- ❑ Escroquerie
- ❑ Racket et extorsion de fonds
- ❑ Contrefaçon et piratage de produits
- ❑ Falsification de documents administratifs et trafic de faux
- ❑ Falsification de moyens de paiement
- ❑ Trafic de substances hormonales et autres facteurs de croissance
- ❑ Blanchiment des produits du crime
- ❑ Faux-monnayage, y compris la contrefaçon de l'euro
- ❑ Cybercriminalité
- ❑ Crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées
- ❑ Aide à l'entrée et au séjour irréguliers
- ❑ Homicide volontaire, coups et blessures graves
- ❑ Trafic d'organes et de tissus humains
- ❑ Enlèvement, séquestration et prise d'otage
- ❑ Racisme et xénophobie
- ❑ Trafic de matières nucléaires ou radioactives
- ❑ Trafic de véhicules volés
- ❑ Viol
- ❑ Incendie volontaire
- ❑ Crimes relevant de la Cour pénale internationale
- ❑ Détournement d'aéronef ou de navire
- ❑ Sabotage

→ L'infraction relève donc de l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI→ L'article 4, paragraphe 1 (demandes urgentes) et paragraphe 3 (demandes non urgentes) de la décision-cadre 2006/960/JAI est donc applicable en ce qui concerne les délais à respecter pour répondre à la présente demande.

Ou

❑ B – L'infraction (les infractions) ne figure(nt) pas dans la liste visée au point A.
Dans ce cas, description de l'infraction(des infractions):

Fins auxquelles les informations ou les renseignements sont demandés

Lien entre les fins auxquelles les informations ou les renseignements sont demandés et la personne qui fait l'objet de ces informations ou de ces renseignements

Identité (dans la mesure où elle est connue) de la (des) personne(s) faisant l'objet principal de l'enquête pénale ou de l'opération de renseignement en matière pénale justifiant la demande d'informations ou de renseignements

Raisons permettant de penser que les informations ou les renseignements se trouvent dans l'État membre requis

Restrictions concernant l'utilisation des informations figurant dans la présente demande à des fins autres que celles pour lesquelles elles ont été fournies ou pour prévenir un danger immédiat et grave pour la sécurité publique

- ❑ L'utilisation est permise.
- ❑ L'utilisation est permise, mais le fournisseur des informations ne doit pas être mentionné.
- ❑ L'utilisation n'est pas permise sans l'autorisation du fournisseur des informations.
- ❑ L'utilisation n'est pas permise

Figure 2

Demandes d'informations et de renseignements

conformément à la décision-cadre 2006/960/JAI

I - Informations administratives

État membre requérant	
Service requérant (nom, adresse, numéro de téléphone, numéro de télécopie, adresse électronique):	
Coordonnées de l'agent chargé du suivi *(facultatif)***:**	
Date et heure de la présente demande:	
Numéro de référence de la présente demande:	
Numéros de référence précédents:	

État(s) membre(s) requis:		
Canal		
☐Officier de liaison UNE/Europol	☐Pour information	☐Pour exécution
☐BCN Interpol	☐Pour information	☐Pour exécution
☐SIRENE	☐Pour information	☐Pour exécution
☐Officier de liaison	☐Pour information	☐Pour exécution
☐Autre (veuillez préciser):	☐Pour information	☐Pour exécution

II - Traitement d'urgence

Traitement d'urgence demandé	☐ Oui ☐ Non
Motifs du traitement d'urgence (par exemple: les suspects sont maintenus en détention, l'affaire doit être portée en justice avant une date déterminée): Application de l'article	
L'infraction relève de l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI relative au mandat d'arrêt européen	☐ Oui ☐ Non

III - Fins

Type de criminalité ou d'activité(s) criminelle(s) faisant l'objet de l'enquête
Description: - des circonstances de la commission de l'infraction (des infractions), (par exemple: le moment, le lieu et le degré de participation à l'infraction (aux infractions) de la personne au sujet de laquelle les informations ou les renseignements sont demandés); - des raisons permettant de penser que les informations ou les renseignements se trouvent dans l'État membre requis; - du lien entre les fins auxquelles les informations ou les renseignements sont demandés et la personne qui fait l'objet de ces informations ou de ces renseignements.
☐ Demande d'utilisation des informations comme preuves si la législation nationale le permet *(facultatif)*

IV - Type d'information

Identité(s) (dans la mesure où elles sont connues) de la (des) personne(s) ou du (des) objet(s)	
Personne	Objet(s)
Nom de famille: Nom à la naissance: Prénom: Date de naissance: Lieu de naissance: Sexe: ☐masculin ☐féminin ☐inconnu Nationalité: Informations supplémentaires:	Numéro de série de l'arme: Numéro du document: Autre numéro d'identification ou nom: Numéro d'immatriculation du véhicule: Numéro de série du véhicule (VIN): Type de documents: Coordonnées de la société (numéro de téléphone, adresse électronique, adresse, site web): Informations supplémentaires:

Informations ou renseignements demandés		
Personne	Véhicule	Autres
☐ vérification de l'identité ☐ recherche dans les bases de données ☐ recherche de l'adresse/du lieu de séjour	☐ données d'identification complémentaires ☐ identification du propriétaire ☐ identification du conducteur ☐ recherche dans les bases de données	☐ identification de la société ☐ recherche de la société dans les bases de données ☐ recherche des documents dans les bases de données ☐ numéro de téléphone/de télécopie ☐ identification du propriétaire de l'adresse électronique ☐ recherche de l'adresse ☐ recherche d'armes ☐ filière de commercialisation des armes
Autres:		

V- Codes de traitement

Restrictions concernant l'utilisation des informations figurant dans la présente demande à des fins autres que celles pour lesquelles elles ont été fournies ou pour prévenir un danger immédiat et grave pour la sécurité publique
☐ à des fins policières uniquement, non pour l'utilisation dans une procédure judiciaire ☐ contacter le fournisseur des informations avant toute utilisation

3.3. Accord de Schengen

3.3.1. Échange de données dans le cadre et en dehors du SIS II

L'accord de Schengen signé le 14 juin 1985 a été complété par la convention d'application de l'accord de Schengen (CAAS)[81] en 1990, qui a créé l'espace Schengen par la suppression des contrôles aux frontières entre les États de l'espace Schengen, l'établissement de règles communes en matière de visas et l'instauration d'une coopération policière et judiciaire. La CAAS définit les exigences générales en matière de coopération policière et autorise les services de police à échanger des informations dans les limites de leurs cadres juridiques nationaux respectifs.

Avec l'entrée en vigueur du traité d'Amsterdam en 1999, des actions de coopération qui relevaient jusqu'alors de Schengen ont été intégrées au cadre juridique de l'Union européenne et les questions liées à Schengen sont désormais traitées par les organes législatifs de l'UE. Le protocole de Schengen annexé au traité d'Amsterdam a fixé des modalités détaillées pour ce processus d'intégration.

Le système d'information Schengen (SIS) a été créé conformément aux dispositions du titre IV de la convention du 19 juin 1990. Il constitue un outil essentiel pour l'application de l'acquis de Schengen. Il s'agit également d'une mesure visant à compenser l'absence de contrôle des personnes aux frontières intérieures dans l'espace Schengen par un outil d'échange d'informations entre les autorités compétentes.

Le fait que le cadre juridique régissant le SIS est actuellement composé d'instruments distincts n'affecte pas le principe selon lequel le SIS constitue un système d'information unique. Les trois nouveaux règlements SIS sont sans incidence sur ce principe. Ils visent à créer des synergies dans la lutte contre le terrorisme et les formes graves de criminalité, notamment en améliorant l'échange d'informations entre les autorités compétentes. Ces règlements contribuent en outre à la gestion des frontières et des migrations et préparent l'interopérabilité du SIS avec les systèmes d'information à grande échelle de l'UE, tels que le VIS, Eurodac, l'ETIAS et l'EES.

---

[81] Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, JO L 239 du 22.9.2000, p. 19.

Législation

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

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

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).

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, JO L 135 du 22.5.2019, p. 27).

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, JO L 135 du 22.5.2019, p. 85.

Principales dispositions

Le système d'information Schengen (SIS) est à la fois un système de coopération policière et de contrôle aux frontières et il appuie la coopération opérationnelle en matière pénale entre les services de police et les autorités judiciaires. Les fonctionnaires de police, gardes-frontières et agents des douanes désignés ainsi que les autorités judiciaires et les autorités chargées des visas dans l'ensemble de l'espace Schengen peuvent consulter le SIS[82].

Le système d'information Schengen de deuxième génération ("SIS II") est actuellement opérationnel dans 26 États membres de l'UE, ainsi que dans les quatre pays tiers qui sont associés à la coopération Schengen: la Norvège, l'Islande, la Suisse et le Liechtenstein.

- En ce qui concerne la coopération policière, le Royaume-Uni et l'Irlande ont tous les deux demandé à être autorisés à participer, mais seul le Royaume-Uni a été autorisé, en 2015, à télécharger des données en temps réel de cette partie du SIS[83], à titre provisoire, comme une première étape permettant la réalisation de l'évaluation avant une décision définitive de mise en œuvre. Le Royaume- Uni et l'Irlande ne participent pas à l'application du SIS aux fins de contrôle aux frontières.

- La Bulgarie, la Roumanie[84] et la Croatie[85] appliquent les dispositions de l'acquis de Schengen relatives à la coopération policière et au contrôle aux frontières. Elles se sont vu accorder un accès en temps réel au SIS afin d'évaluer la bonne application des dispositions de l'acquis de Schengen relatives au SIS. Une fois ces évaluations effectuées d'une manière satisfaisante, une décision distincte du Conseil fixera une date pour la suppression des contrôles aux frontières intérieures. Jusqu'à cette date, certaines restrictions à l'utilisation du SIS sont maintenues.

- Chypre n'a pas encore accès au SIS.

---

82 Une liste consolidée des autorités nationales compétentes, qui indique, pour chaque autorité, les données qu'elle peut consulter et à quelles fins, est publiée chaque année au Journal officiel de l'UE conformément à l'article 31, paragraphe 8, du règlement SIS II et à l'article 46, paragraphe 8, de la décision SIS II.

83 Décision d'exécution (UE) 2015/215 du Conseil du 10 février 2015 relative à la mise en œuvre des dispositions de l'acquis de Schengen concernant la protection des données et à la mise en œuvre provisoire de certaines parties des dispositions de l'acquis de Schengen concernant le Système d'information Schengen au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, JO L 36 du 12.2.2015, p. 8.

84 Décision 2010/365/EU du Conseil du 29 juin 2010 sur l'application à la République de Bulgarie et à la Roumanie des dispositions de l'acquis de Schengen relatives au système d'information Schengen, JO L 166 du 1.7.2010, p. 17.

85 Décision (UE) 2017/733 du Conseil du 25 avril 2017 sur l'application en République de Croatie des dispositions de l'acquis de Schengen relatives au système d'information Schengen, JO L 108 du 26.4.2017, p. 31.

Les données du SIS II peuvent être consultées en ligne (sous réserve du respect de règles strictes en matière de protection des données) 24 heures sur 24 et 7 jours sur 7 par l'intermédiaire des bureaux SIRENE, dans les points de contrôle des frontières, sur le territoire national et auprès des consulats à l'étranger. Les données prennent la forme de signalements, un signalement étant un ensembles de données qui permettent aux autorités d'identifier des **personnes**, c'est-à-dire des citoyens européens ou des ressortissants de pays tiers, ou des **objets** en vue de prendre les mesures appropriées aux fins de la lutte contre la criminalité et l'immigration clandestine.

Plus précisément, le personnel autorisé d'Europol a le droit, dans les limites de son mandat, d'accéder directement aux données introduites dans le SIS II et de les consulter, et il peut demander des informations supplémentaires à l'État membre concerné.

Les membres nationaux d'Eurojust et leurs assistants ont le droit, dans les limites de leur mandat, d'accéder aux données introduites dans le SIS II et de les consulter.

Conformément à l'article 47 de la CAAS, les officiers de liaison détachés auprès des autorités de police dans d'autres États Schengen ou des pays tiers sont chargés de l'échange d'informations en application:

- de l'article 39, paragraphes 1, 2 et 3 dans le respect du droit national, à des fins de prévention et de détection des infractions pénales;

- de l'article 46, même de leur propre initiative, aux fins de la prévention d'infractions portant atteinte à l'ordre et à la sécurité publics, ainsi que de menaces à cet égard.

Il convient de noter que les dispositions de l'article 39, paragraphes 1, 2 et 3, et de l'article 46, dans la mesure où elles ont trait à l'échange d'informations ou de renseignements concernant des infractions graves, sont remplacées par celles de la décision-cadre 2006/960/JAI du Conseil, la "décision-cadre suédoise". Toutefois, les dispositions de l'article 39, paragraphes 1, 2 et 3, et de l'article 46, restent applicables à l'égard des infractions punissables d'une peine d'emprisonnement de douze mois ou moins.

3.3.2. Refonte du système d'information Schengen

Législation

Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).

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).

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).

Principales dispositions

Trois ans après la mise en service du SIS II, la Commission a procédé à une évaluation du système. La refonte du SIS II tient compte de cette évaluation et de la participation distincte des États membres de l'UE aux politiques de l'UE relatives à l'espace de liberté, de sécurité et de justice. Les trois règlements apportent un ensemble d'améliorations au SIS qui le rendront plus efficace, renforceront la protection des données et élargiront les droits d'accès. Ces règlements contribuent en outre à la gestion des frontières et des migrations et préparent l'interopérabilité du SIS avec les systèmes d'information à grande échelle de l'UE[86].

Les règlements contiennent des règles spécifiques concernant les États membres qui ont un statut particulier pour ce qui est de Schengen et des mesures relatives à l'espace de liberté, de sécurité et de justice adoptées dans le cadre du TFUE, à savoir le Danemark, l'Irlande, la Croatie, la Bulgarie, la Roumanie et Chypre.

---

[86] 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 (JO L 135 du 22.5.2019, p. 85).

Les dispositions du règlement 2018/1862 relatives au fonctionnement et à l'utilisation du SIS aux fins de la coopération policière et judiciaire en matière pénale concernent, en particulier:

- les nouvelles catégories de signalements, tant pour les personnes, telles que les "personnes recherchées inconnues" et le "contrôle d'investigation", l'extension de la catégorie "personnes disparues" aux "personnes vulnérables qui doivent être empêchées de voyager", que pour les objets, tels que les "objets de grande valeur";

- l'obligation pour les États membres de créer des signalements SIS pour les cas liés à des infractions terroristes;

- les règles relatives aux informations à communiquer à Europol en cas de réponses positives à des signalements liés à des infractions terroristes;

- les règles relatives à l'utilisation, à des fins d'identification, de données biométriques, telles que les images faciales et les photographies lorsque cela est techniquement possible[87], les empreintes digitales, les empreintes palmaires et, en particulier, les profils ADN, uniquement pour l'identification de personnes disparues;

- les droits d'accès à des fins répressives en ce qui concerne les autorités chargées de l'immigration, les services chargés de l'immatriculation des bateaux et des aéronefs, et les services chargés de l'enregistrement des armes à feu; le droit d'accès complet d'Europol au SIS, y compris en ce qui concerne les personnes disparues, les signalements concernant les retours et les signalements concernant des ressortissants de pays tiers, et son droit d'échanger et de demander des informations supplémentaires conformément aux dispositions du manuel Sirene; les droits d'accès accordés à l'Agence européenne de garde-frontières et de garde-côtes (Frontex) et à ses équipes, dans la mesure où cela est nécessaire à l'exécution de leurs missions et où cela est requis par le plan opérationnel pour une opération spécifique de garde-frontières;

- le renforcement de la protection et de la sécurité des données grâce à l'introduction de garanties supplémentaires visant à assurer que la collecte et le traitement des données, ainsi que l'accès à celles-ci, sont limités à ce qui est strictement nécessaire et requis sur le plan opérationnel, à l'application du cadre de l'UE en matière de protection des données, en particulier la directive 2016/680 et le RGPD, et à la coordination et à la surveillance de bout en bout par les autorités nationales chargées de la protection des données et le Contrôleur européen de la protection des données.

---

[87] Les images faciales et les photographies ne devraient dans un premier temps être utilisées, à des fins d'identification, que dans le contexte des points de passage frontaliers habituels. Une telle utilisation devrait faire l'objet d'un rapport de la Commission confirmant que la technique requise est disponible, fiable et prête à être employée. À un stade ultérieur, la Commission pourrait adopter des actes concernant la détermination des circonstances dans lesquelles des photographies et des images faciales peuvent être utilisées aux fins de l'identification de personnes dans un contexte autre que celui des points de passage frontaliers habituels.

3.4. Europol

Législation

Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à compter du 1er mai 2017).

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

Principales dispositions

L'objectif d'Europol est de soutenir et de renforcer l'action des autorités compétentes des États membres chargées de la prévention de la criminalité et de la lutte contre celle-ci, ainsi que leur coopération mutuelle pour prévenir et combattre la criminalité organisée, le terrorisme et d'autres formes graves de criminalité affectant deux États membres ou plus. À cette fin, Europol recueille, stocke, traite, analyse et échange des informations et des renseignements en matière pénale.

Chaque État membre désigne une unité nationale (UNE) qui fonctionne comme un organe de liaison entre Europol et les autorités compétentes dans les États membres. Les UNE accomplissent des tâches liées au partage d'informations et de renseignements pertinents. Chaque unité nationale détache au moins un officier de liaison qui constitue le bureau national de liaison auprès d'Europol et représente les intérêts de ladite unité nationale. Les officiers de liaison sont chargés de l'échange d'informations entre, d'une part, les États membres et Europol et, d'autre part, de manière bilatérale entre les autres pays. Ces échanges bilatéraux peuvent porter sur des infractions sortant du mandat d'Europol.

Le règlement Europol introduit un nouveau concept pour le traitement des données, communément appelé le concept de gestion intégrée des données ("Integrated Data Management Concept"). Ce concept peut être défini comme étant la possibilité d'utiliser des informations relatives à des activités criminelles afin de les exploiter de diverses manières conformément à ce qu'a indiqué le propriétaire des données, ce qui permet de les gérer et de les traiter d'une manière intégrée technologiquement neutre. En vertu de la décision du Conseil portant création d'Europol, le traitement des données s'articulait autour de systèmes. Le règlement Europol ne contient plus de références à des systèmes mais requiert d'indiquer à quelles fins les données sont traitées. Afin de faciliter une transition en douceur, les utilisateurs peuvent continuer à travailler avec les systèmes existants en le faisant d'une manière conforme au nouveau cadre juridique.

L'unité nationale est responsable de la communication avec le système d'information Europol (SIE) utilisé pour traiter les données nécessaires à l'exécution des tâches d'Europol. L'unité nationale, les officiers de liaison et le personnel d'Europol dûment autorisé ont le droit de saisir des données dans les systèmes et d'en extraire des données. Les informations introduites dans le SIE sont généralement considérées comme étant fournies à des fins de recoupement (article 18, paragraphe 2, point a), du règlement) et d'analyse de nature stratégique ou thématique (article 18, paragraphe 2, point b), du règlement).

3.5. Agence européenne de garde-frontières et de garde-côtes (Frontex)

Législation

Règlement (UE) 2019/1896 du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes (JO L 295 du 14.11.2019, p. 1) et abrogeant les règlements (UE) n° 1052/2013 et (UE) 2016/1624 (applicable à partir du 4 décembre 2019).

Le règlement (UE) n° 1052/2013 portant création du système européen de surveillance des frontières (Eurosur) prévoit "un cadre commun pour l'échange d'informations et pour la coopération entre les États membres et Frontex en vue d'améliorer la connaissance de la situation et d'accroître la capacité de réaction aux frontières extérieures des États membres de l'Union (ci-après dénommées "frontières extérieures") aux fins de détecter, prévenir et combattre l'immigration illégale et la criminalité transfrontalière et de contribuer à assurer la protection de la vie des migrants et à leur sauver la vie (ci-après dénommé "EUROSUR")". Le règlement EUROSUR a été abrogé et remplacé par le règlement (UE) 2019/1896, qui contient des dispositions révisées concernant EUROSUR.

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

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 19.09.2018, p. 1.

Principales dispositions

Le corps européen de garde-frontières et de garde-côtes a pour objectif d'assurer une gestion européenne intégrée des frontières extérieures dans le but de gérer efficacement ces frontières, dans le plein respect des droits fondamentaux, et d'accroître l'efficacité de la politique de l'Union en matière de retour.

L'Agence européenne de garde-frontières et de garde-côtes (Frontex, ci-après dénommée l'"Agence") s'occupe des défis migratoires et des éventuels futurs problèmes et menaces aux frontières extérieures. En vue de prévenir, détecter et combattre la criminalité transfrontalière aux frontières extérieures, l'Agence assure un niveau élevé de sécurité intérieure au sein de l'Union, dans le plein respect des droits fondamentaux, tout en préservant la libre circulation des personnes dans l'Union.

Chaque État membre désigne un point de contact national chargé de la communication avec l'Agence sur toutes les questions relatives aux activités menées par celle-ci, sans préjudice du rôle des centres nationaux de coordination. Les États membres peuvent désigner jusqu'à deux membres du personnel représentant leur point de contact national pour être affectés auprès de l'Agence en tant qu'officiers de liaison.

Chacun des États membres désigne, met en service et gère un centre national de coordination, qui assure la coordination et l'échange d'informations entre toutes les autorités chargées du contrôle aux frontières extérieures au niveau national ainsi qu'avec les autres centres nationaux de coordination et l'Agence.

Le règlement relatif au corps européen de garde-frontières et de garde-côtes met en place EUROSUR en tant que cadre intégré pour l'échange d'informations et pour la coopération opérationnelle au sein du corps européen de garde-frontières et de garde-côtes. Il vise à améliorer la connaissance de la situation et à accroître la capacité de réaction aux fins de la gestion des frontières, en vue de prévenir, détecter et combattre l'immigration illégale et la criminalité transfrontalière, ainsi que de protéger et de sauver la vie des migrants. L'Agence coordonne les services de fusion d'EUROSUR, afin que les centres nationaux de coordination, la Commission et l'Agence elle-même reçoivent de manière régulière, fiable et efficiente en termes de coûts des informations relatives aux frontières extérieures et à la zone située en amont des frontières.

Aux fins de la mise en œuvre du règlement ETIAS, l'Agence assurera la création de l'unité centrale ETIAS. Cette unité, opérationnelle 24 heures sur 24 et 7 jours sur 7, est chargée de vérifier, dans les cas où le traitement automatisé de la demande a donné lieu à une réponse positive, si les données à caractère personnel du demandeur correspondent aux données à caractère personnel de la personne ayant déclenché cette réponse positive. Lorsqu'une réponse positive est confirmée ou qu'il subsiste des doutes à ce sujet, l'unité centrale ETIAS devrait lancer le traitement manuel de la demande. Aux fins de la mise en œuvre du règlement sur l'interopérabilité, pendant une période d'un an suivant la notification par l'eu-LISA de l'achèvement de l'essai du détecteur d'identités multiples (MID), et avant la mise en service du MID, l'unité centrale ETIAS est responsable de la détection d'identités multiples à l'aide des données stockées dans l'EES, le VIS, Eurodac et le SIS.

Aux fins de la mise en œuvre du mandat de l'Agence européenne de garde-frontières et de garde-côtes (Frontex), celle-ci a examiné comment les informations reçues avant l'arrivée (informations préalables) d'un voyageur aux frontières extérieures pouvaient être utilisées pour affiner l'analyse des risques liés aux voyageurs. L'accent a été mis sur l'étude des capacités existantes et le recensement de nouvelles méthodes permettant d'optimiser cette analyse, dans le but d'améliorer le processus de prise de décision lors du franchissement des frontières tout en simplifiant davantage les procédures pour les voyageurs de bonne foi.

Les lignes directrices sur l'information préalable contribuent à l'élaboration de profils afin de mieux détecter en amont les voyageurs présentant un intérêt, ainsi qu'au renforcement des capacités de ciblage. Frontex a lancé une session de formation portant spécifiquement sur les informations préalables afin d'aider les États membres à mettre en place des capacités d'analyse harmonisées ("capacités de ciblage") aux fins de la gestion des frontières.

En outre, une étude lancée en janvier 2020 examine l'utilisation des informations préalables concernant les voyageurs entrant dans l'espace Schengen par les frontières extérieures terrestres et maritimes. L'un des principaux objectifs de cette étude est de recenser, décrire et définir les bonnes pratiques en matière de collecte et de traitement de ces informations préalables.

3.6. Interpol

Législation

Constitution d'Interpol[88]

Règles régissant le traitement des informations[89]

Règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol

Principales dispositions

La mission d'Interpol consiste à faciliter la coopération policière internationale en vue de prévenir et de combattre la criminalité grâce à une coopération renforcée et à des innovations en matière de police et de sécurité. Des mesures sont prises dans les limites de la législation en vigueur dans les États membres et dans l'esprit de la Déclaration universelle des droits de l'homme. Chacun des 190 États membres dispose d'un bureau central national (BCN) dont le fonctionnement est assuré par ses propres agents, très bien formés, des services répressifs.

La Constitution d'Interpol est un accord international qui confirme, en tant que membres, les gouvernements de tous les pays qui ont participé à son adoption en 1956 et établit la procédure de candidature permettant aux pays non membres en 1956 de rejoindre Interpol.

---

88 http://www.interpol.int/fr/À-propos-d'INTERPOL/Documents-juridiques/The-Constitution

89 http://www.interpol.int/fr/À-propos-d'INTERPOL/Documents-juridiques/Fundamental-texts

En tant que principal document juridique, la Constitution expose les buts et les objectifs d'Interpol. Elle définit le mandat de l'organisation qui est d'assurer la coopération la plus large possible entre toutes les autorités de police criminelle, ainsi qu'en matière de répression des infractions de droit commun.

En plus de la Constitution, un certain nombre de textes fondamentaux constituent le cadre juridique d'Interpol. Plusieurs niveaux de contrôle ont été mis en place afin d'assurer le respect des règles. Ces niveaux concernent les contrôles effectués par les bureaux centraux nationaux (BCN), par le Secrétariat général et par l'organisme de contrôle indépendant connu sous le nom de Commission de contrôle des fichiers d'Interpol (CCF).

3.7. Officiers de liaison

Législation

Convention d'application de l'Accord de Schengen du 19 juin 1990 (CAAS)[90], article 47

Décision 2003/170/JAI du Conseil du 27 février 2003 relative à l'utilisation commune des officiers de liaison détachés par les autorités répressives des États membres[91]

Décision 2006/560/JAI du Conseil du 24 juillet 2006 modifiant la décision 2003/170/JAI relative à l'utilisation commune des officiers de liaison détachés par les autorités répressives des États membres[92]

Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53 (applicable à partir du 1er mai 2017)

Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210 du 6.8.2008, p. 1

Accords bilatéraux

---

90 Convention d'application de l'Accord de Schengen du 19 juin 1990 (CAAS), JO L 239 du 22.9.2000, p. 19.

91 Décision du Conseil 2003/170/JAI du 27 février 2003, JO L 67 du 12.3.2003, p. 27.

92 Décision du Conseil 2006/560/JAI du 24 juillet 2006, JO L 219 du 10.8.2006, p. 31.

Principales dispositions

L'article 47 de la CAAS prévoit que les États membres "peuvent conclure des accords bilatéraux permettant le détachement, pour une durée déterminée ou indéterminée, de fonctionnaires de liaison (...) [d'un État membre] auprès de services de police de l'autre (...) [État membre]". Les officiers de liaison ne sont pas habilités à appliquer des mesures de police de manière autonome et l'article 47 précise que de tels détachements ont "pour but de promouvoir et d'accélérer la coopération (...), notamment en accordant l'assistance:

a) sous la forme d'échange d'informations aux fins de la lutte tant préventive que répressive contre la criminalité;

b) dans l'exécution de demandes d'entraide policière et judiciaire en matière pénale;

c) pour les besoins de l'exercice des missions des autorités chargées de la surveillance des frontières extérieures."

De plus amples informations concernant de tels détachements figurent dans le "Manuel concernant les matchs de football"[93] et dans la recommandation du Conseil du 6 décembre 2007 relative à un Manuel destiné aux autorités de police et de sécurité concernant la coopération lors d'événements majeurs revêtant une dimension internationale[94].

La disposition du CAAS selon laquelle les officiers de liaison nationaux représentent également les intérêts d'un ou de plusieurs autres États membres a été complétée par la décision du Conseil relative à l'utilisation commune des officiers de liaison détachés par les services répressifs des États membres (décision modifiée en 2006). Une disposition a également été prévue pour renforcer la coopération entre les officiers de liaison de différents États membres sur leur lieu de détachement. Dans plusieurs enceintes, il a été souligné que cette coopération devait être encouragée.

---

93 Résolution du Conseil concernant un manuel actualisé assorti de recommandations pour la mise en place, à l'échelle internationale, d'une coopération policière et de mesures visant à prévenir et à maîtriser la violence et les troubles liés aux matchs de football revêtant une dimension internationale qui concernent au moins un État membre ("manuel de l'Union européenne concernant les matchs de football"), JO C 444 du 29.11.2016, p. 1.

94 JO C 314 du 22.12.2007, p. 4.

Conformément au règlement Europol, chaque État membre désigne une unité nationale (UNE) qui sert d'organe de liaison entre Europol et les autorités compétentes des États membres chargées de la prévention des infractions pénales et de la lutte contre celles-ci. Les UNE accomplissent des tâches liées au partage d'informations et de renseignements pertinents. Chaque unité nationale détache au moins un officier de liaison qui constitue le bureau national de liaison auprès d'Europol et représente les intérêts de ladite unité nationale. Les officiers de liaison sont chargés de l'échange d'informations entre, d'une part, l'unité nationale et Europol et, d'autre part, de manière bilatérale entre les autres unités nationales. Ces échanges bilatéraux peuvent porter sur des infractions sortant du mandat d'Europol.

La décision 2008/615/JAI du Conseil ("décision Prüm") prévoit, à ses articles 17 et 18, le détachement d'agents nationaux aux fins de maintenir l'ordre et la sécurité publics et de prévenir les infractions pénales.

3.8. Échange de données Prüm

Législation

- Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière

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

Principales dispositions

Les États membres s'accordent mutuellement un accès transfrontière en ligne aux données de référence des fichiers nationaux d'analyse ADN et des systèmes de reconnaissance automatisée d'empreintes digitales (AFIS), ainsi qu'aux données d'immatriculation des véhicules (DIV) (voir chapitre 2 de la décision 2008/615/JAI du Conseil).

Des PCN spécifiques doivent être désignés dans chaque État membre. Les dispositions en matière de protection et de sécurité des données doivent être dûment prises en considération dans la législation nationale. La comparaison automatisée de profils biométriques anonymes s'appuie sur un système "hit - no hit", sauf dans le cas des DIV pour lesquelles le propriétaire/détenteur du véhicule faisant l'objet de la recherche est automatiquement indiqué en réponse.

En cas de correspondance biométrique, le PCN de l'État membre qui effectue la consultation reçoit, dans le cadre d'un processus automatisé, les données de référence pour lesquelles une concordance a été trouvée.

Des données à caractère personnel supplémentaires bien précises et des informations complémentaires relatives aux données de référence peuvent être demandées par le biais de procédures d'entraide judiciaire, notamment celles adoptées conformément à la "décision-cadre suédoise".

La fourniture de telles données supplémentaires est régie par le droit national de l'État membre requis, y compris les dispositions relatives à l'entraide judiciaire. Il est entendu que la transmission de données à caractère personnel suppose un niveau adéquat de protection des données de la part de l'État membre destinataire[95].

Aux fins de la prévention des infractions pénales et dans l'intérêt du maintien de l'ordre et de la sécurité publics en liaison avec des manifestations de grande envergure revêtant une dimension transfrontière, les États membres peuvent, à la fois sur demande ou de leur propre initiative, se transmettre les uns aux autres des données à caractère non personnel, ainsi qu'à caractère personnel. À cette fin, des points de contact nationaux (PCN) spécifiques sont désignés (voir chapitre 3 de la décision 2008/615/JAI du Conseil).

Aux fins de la prévention des infractions terroristes, les États membres peuvent se transmettre les uns aux autres des données à caractère personnel dans certaines circonstances. À cette fin, des points de contact nationaux spécifiques sont désignés (voir chapitre 4 de la décision 2008/615/JAI du Conseil).

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

Législation

Décision 2004/512/CE du Conseil du 8 juin 2004 portant création du système d'information sur les visas (VIS), JO L 213 du 15.6.2004, p. 5.

---

[95] La décision 2008/615/JAI du Conseil respecte le niveau de protection prévu pour le traitement des données à caractère personnel dans la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et dans son protocole additionnel du 8 novembre 2001, ainsi que les principes énoncés dans la recommandation n° R (87) 15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

Décision 2013/392/UE du Conseil fixant la date de prise d'effet de la décision 2008/633/JAI concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 198 du 23.7.2013, p. 45[96].

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

Principales dispositions

Le VIS est un système qui permet aux autorités nationales compétentes de saisir et d'actualiser des données relatives aux visas de court séjour (visas Schengen) ainsi que de consulter celles-ci par voie électronique. Il s'appuie sur une architecture centralisée et comprend un système d'information central, le système central d'information sur les visas (CS-VIS), une interface nationale dans chaque État membre (NI-VIS) et l'infrastructure de communication entre le CS-VIS et les NI-VIS. La décision 2008/633/JAI permet d'utiliser le VIS pour prévenir et détecter les infractions terroristes et d'autres infractions pénales graves, et mener des enquêtes en la matière. Elle habilite les autorités répressives désignées dans les pays de l'espace Schengen (notamment les autorités chargées de lutter contre le terrorisme ou les infractions pénales graves, par exemple le trafic de drogue ou la traite des êtres humains), ainsi qu'Europol à avoir accès au VIS. Les autorités nationales désignées doivent suivre une procédure pour accéder au VIS une fois que toutes les conditions d'accès sont remplies.

---

96 Le 16 avril 2015, la Cour de justice de l'Union européenne a annulé la décision 2013/392/UE du Conseil fixant la date de prise d'effet de la décision 2008/633/JAI concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. Toutefois, la Cour a déclaré que les effets de la décision 2013/392 seraient maintenus jusqu'à l'entrée en vigueur d'un nouvel acte appelé à la remplacer.

En mai 2018, la Commission a présenté une proposition législative modifiant le règlement VIS qui vise notamment à assurer l'interopérabilité entre d'autres bases de données dans le domaine de la justice et des affaires intérieures, en enregistrant dans le VIS les visas de long séjour et les titres de séjour. En outre, la proposition incorpore et précise les règles régissant l'accès des autorités répressives au VIS, tout en abrogeant la décision 2008/633/JAI.

La version améliorée du VIS ne devrait pas être opérationnelle avant la fin de 2021.

3.10. Eurodac

Législation

Le système de reconnaissance automatisée d'empreintes digitales (Eurodac) est un système informatique visant initialement à faciliter l'application effective de la convention de Dublin. La convention de Dublin, signée le 15 juin 1990, a été remplacée par le règlement (CE) n° 343/2003 du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers.

À la suite des modifications apportées aux règlements relatifs à Eurodac, ceux-ci ont été refondus par les actes suivants:

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

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) nº 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 (JO L 135 du 22.5.2019, p. 27)

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 (JO L 135 du 22.5.2019, p. 85)

Principales dispositions

Le règlement (UE) n° 603/2013 expose l'objectif d'Eurodac et définit les conditions d'accès des autorités répressives nationales désignées et d'Europol aux données d'Eurodac aux fins de la prévention ou de la détection des infractions terroristes[97] ou d'autres infractions pénales graves[98], et des enquêtes en la matière.

3.11. Naples II

Législation

Acte du Conseil du 18 décembre 1997 établissant, sur la base de l'article K.3 du traité sur l'Union européenne, la convention relative à l'assistance mutuelle et à la coopération entre les administrations douanières, publié au JO C 24 du 23.1.1998, p. 1

---

97 Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, JO L 164 du 22.6.2002, p. 3.

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

Principales dispositions

Les États membres se prêtent assistance mutuelle en vue de prévenir et de détecter les infractions aux réglementations douanières nationales, ainsi que de poursuivre et de réprimer les infractions aux réglementations douanières communautaires et nationales. En ce qui concerne les enquêtes pénales, la convention Naples II établit les procédures dans le cadre desquelles les administrations douanières peuvent agir conjointement et s'échanger des données, spontanément ou sur demande, en matière de trafics illicites.

Les demandes sont soumises par écrit dans une langue officielle de l'État membre de l'autorité requise ou dans une langue acceptée par cette autorité. Un formulaire fixe la norme en matière de communication d'informations. Les autorités concernées communiquent toutes les informations susceptibles d'aider à prévenir, à détecter et à poursuivre les infractions. Elles échangent des données à caractère personnel, à savoir toutes les informations qui se rapportent à une personne physique identifiée ou identifiable.

Dans le cadre de l'assistance prêtée, l'autorité requise, ou l'autorité compétente saisie par cette dernière, procède comme si elle agissait pour son propre compte ou à la demande d'une autre autorité de son propre État membre.

3.11.1. Système d'information douanier - SID[99]

Le système d'information douanier complète la Convention Naples II[100]. Le système d'information centralisé est géré par la Commission et vise à renforcer l'administration douanière des États membres grâce à un échange d'informations rapide, en vue de prévenir les infractions graves aux lois nationales et communautaires, d'enquêter sur elles et de les poursuivre. Le SID met également en place un fichier d'identification des dossiers (FIDE) afin d'assister les enquêtes douanières.

---

99 Décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes, JO L 323 du 10.12.2009, p. 20.

100 Convention établie sur la base de l'article K.3 du traité sur l'Union européenne, relative à l'assistance mutuelle et à la coopération entre les administrations douanières, JO C 24 du 23.1.1998, p. 2.

Les autorités désignées par les États membres[101] ont directement accès aux données contenues dans le SID. Afin de renforcer leur complémentarité avec Europol et Eurojust, les deux organes se voient accorder un accès en lecture seule au SID et au FIDE.

Le SID comprend les données à caractère personnel se rapportant à des marchandises, moyens de transports, entreprises, personnes et retenues, saisies ou confiscations d'articles et d'argent liquide. Les données à caractère personnel ne peuvent être copiées du SID dans d'autres systèmes de traitement des données qu'à des fins d'analyses opérationnelles ou de gestion des risques, et seuls les analystes désignés par les États membres peuvent y accéder.

Le FIDE permet aux autorités nationales chargées de mener des enquêtes en matière douanière, lorsqu'elles ouvrent un dossier d'enquête, d'identifier les autres autorités qui auraient pu enquêter sur une personne ou une entreprise donnée.

3.12. Bureaux de recouvrement des avoirs (BRA) et réseau CARIN

Législation

Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime, JO L 332 du 18.12.2007, p. 103

Le Réseau Camden regroupant les autorités compétentes en matière de recouvrement d'avoirs (CARIN) a été mis en place à La Haye les 22 et 23 septembre 2004 par l'Autriche, la Belgique, l'Allemagne, l'Irlande, les Pays-Bas et le Royaume-Uni.

[101] Mise en œuvre de l'article 7, paragraphe 2, et de l'article 8, paragraphe 3, de la décision 2009/917/JAI du Conseil du 30 novembre 2009 sur l'emploi de l'informatique dans le domaine des douanes - listes actualisées des autorités compétentes, doc. 13394/11 ENFOCUSTOM 85.

Principales dispositions

À la suite de l'adoption de la décision 2007/845/JAI du Conseil[102], tous les États membres ont depuis mis en place et désigné des bureaux de recouvrement des avoirs (BRA). Ceux-ci peuvent s'échanger directement des informations sur les questions relatives au recouvrement des avoirs en ayant recours au système SIENA. Sous l'égide de la Commission européenne et d'Europol, le réseau des BRA facilite la coopération entre les bureaux de recouvrement des avoirs des États membres, ainsi que la discussion stratégique et l'échange de bonnes pratiques. Le Bureau des avoirs d'origine criminelle d'Europol (ECAB, "Europol Criminal Assets Bureau") joue un rôle de coordination dans le cadre du recouvrement des avoirs au sein de l'UE.

Les dispositions fixées par la directive 2014/42/UE du Parlement européen et du Conseil du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne[103] permettront de poursuivre le renforcement de l'efficacité de la coopération entre les bureaux de recouvrement des avoirs au sein de l'Union européenne. Les États membres sont invités à transposer la directive au plus tard le 4 octobre 2016.

Le Réseau Camden regroupant les autorités compétentes en matière de recouvrement d'avoirs (CARIN), mis en place en 2004 en appui à l'identification, au gel, à la saisie et à la confiscation transfrontières de biens en rapport avec le crime, renforce l'échange mutuel d'informations en ce qui concerne différentes approches nationales dont la portée s'étend au-delà de l'UE.

Depuis 2015, le réseau CARIN comprend des praticiens de 53 juridictions et de 9 organisations internationales, qui servent de points de contact aux fins d'échange transfrontière rapide d'informations, sur demande ou de manière spontanée. Les BRA nationaux coopèrent entre eux ou avec d'autres autorités qui facilitent le dépistage et l'identification des produits du crime. Si tous les États membres ont mis en place leur BRA, il existe néanmoins de grandes différences entre les États membres en termes d'organisation, de ressources et d'activités.

---

102 Décision 2007/845/JAI du Conseil du 6 décembre 2007 relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d'identification des produits du crime ou des autres biens en rapport avec le crime, JO L 332 du 18.12.2007, p. 103.

103 Directive 2014/42/UE du Parlement européen et du Conseil du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne, JO L 127 du 29.4.2014, p. 39.

Les informations échangées peuvent être utilisées conformément aux dispositions en matière de protection des données de l'État membre destinataire et sont soumises aux mêmes règles de protection des données que si elles avaient été recueillies dans l'État membre destinataire. L'échange spontané d'informations effectué conformément à cette décision, en appliquant les procédures et délais prévus par la décision-cadre suédoise, doit être encouragé.

3.13. Cellules de renseignement financier (CRF)

Législation

Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, JO L 141 du 5.6.2015, p. 73

Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil, JO L 186 du 11.7.2019, p. 122

Principales dispositions

Conformément à la directive (UE) 2015/849 (la quatrième directive sur la lutte contre le blanchiment de capitaux, modifiée par la directive (UE) 2018/843), chaque État membre met en place une CRF, chargée de prévenir, de détecter et de combattre efficacement le blanchiment de capitaux et le financement du terrorisme. En sa qualité de cellule nationale centrale, la CRF est chargée de recevoir et d'analyser les déclarations de transactions suspectes ainsi que d'autres informations pertinentes concernant le blanchiment de capitaux, les infractions sous-jacentes associées ou le financement du terrorisme. La CRF est chargée de disséminer les résultats de ses analyses aux autorités compétentes, ainsi que toute autre information pertinente, lorsqu'il existe des raisons de suspecter un blanchiment de capitaux, des infractions sous-jacentes associées ou un financement du terrorisme. Elle est en mesure d'obtenir des informations complémentaires auprès des entités assujetties. Les CRF sont en mesure de donner suite aux demandes d'informations soumises par les autorités compétentes de leur État membre respectif lorsque ces demandes d'informations sont motivées par des préoccupations liées au blanchiment des capitaux, à des infractions sous-jacentes associées ou au financement du terrorisme.

Outre l'échange d'informations concernant le blanchiment des capitaux et le financement du terrorisme, la directive (UE) 2019/1153 prévoit que chaque État membre veille à ce que sa CRF soit également tenue de coopérer avec ses autorités compétentes désignées et d'être en mesure de donner suite aux demandes d'informations financières ou d'analyses financières présentées par ces autorités compétentes et motivées par des préoccupations liées à la prévention ou à la détection des infractions pénales graves définies à l'annexe I du règlement Europol (2016/794), ou aux enquêtes ou poursuites en la matière.

Dans les deux cas, la CRF peut refuser de communiquer les informations demandées lorsqu'il existe des raisons objectives de supposer que cela aurait une incidence négative sur des enquêtes en cours, ou lorsque la divulgation des informations serait manifestement disproportionnée par rapport aux intérêts légitimes d'une personne physique ou morale ou ne serait pas pertinente par rapport aux finalités pour lesquelles elles ont été demandées.

Conformément à la directive (UE) 2015/849, les États membres veillent à ce que les CRF échangent entre elles, spontanément ou sur demande, toute information susceptible d'être pertinente pour le traitement ou l'analyse d'informations effectués par la CRF concernant le blanchiment de capitaux ou le financement du terrorisme et la personne physique ou morale impliquée, quel que soit le type d'infraction sous-jacente associée et même si le type d'infraction sous-jacente associée n'est pas identifié au moment où l'échange se produit. Une CRF ne peut refuser d'échanger des informations qu'à titre exceptionnel, lorsque l'échange pourrait être contraire à des principes fondamentaux de son droit national. Les États membres veillent à ce que les informations échangées en application des articles 52 et 53 de la directive soient utilisées uniquement aux fins pour lesquelles elles ont été demandées ou fournies.

Au-delà des échanges entre les CRF de différents États membres conformément à la directive 2015/849, la directive 2019/1153 prévoit à présent que, dans des cas exceptionnels et urgents, les CRF sont en outre habilitées à échanger des informations financières ou des analyses financières susceptibles d'être pertinentes pour le traitement ou l'analyse d'informations liées au terrorisme ou à la criminalité organisée associée au terrorisme. La directive 2019/1153 autorise aussi l'échange d'informations entre les CRF et Europol.

CRF.NET est un réseau informatique décentralisé d'échange d'informations entre CRF.

Ce réseau CRF.NET, qui visait initialement à renforcer la position des CRF, a été développé au cours des dernières années, transformant un outil de base sécurisé pour l'échange bilatéral structuré d'informations en un outil multifonctionnel sécurisé pour l'échange multilatéral d'informations prévoyant des fonctionnalités de gestion des dossiers ainsi qu'une normalisation semi-automatisée des processus. Dans CRF.NET, chaque nouvelle fonctionnalité et chaque nouveau processus automatisé sont facultatifs et ne sont assortis d'aucune restriction. Les différentes CRF peuvent décider quels sont les possibilités et fonctionnalités de CRF.NET qu'elles utilisent; elles n'ont recours qu'aux fonctionnalités qui leur conviennent et excluent celles dont elles n'ont pas besoin ou auxquelles elles n'ont pas envie de faire appel.

3.14. Accord UE/États-Unis sur le programme de surveillance du financement du terrorisme (TFTP)

Législation

Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO L 195 du 27.7.2010, p. 5

Principales dispositions

Au lendemain du 11 septembre, l'UE et les États-Unis ont décidé de coopérer étroitement et ont conclu l'accord sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (accord TFTP entre l'UE et les États-Unis). À la suite de l'accord, le département du Trésor des États-Unis met également des informations TFTP à la disposition des services répressifs des États membres concernés, de leurs organismes chargés de la sécurité publique ou de leurs autorités chargées de la lutte contre le terrorisme, ainsi que, le cas échéant, d'Europol et d'Eurojust.

Le TFTP prévoit de solides mesures de contrôle afin de veiller au respect des garanties, y compris de celles relatives à la protection des données à caractère personnel. Les données sont traitées exclusivement aux fins de prévenir les actes terroristes ou leur financement, d'enquêter en la matière, de les détecter ou de les poursuivre. Aux fins dudit accord, le département du Trésor des États-Unis peut demander des données de messagerie financière et des données connexes qui sont stockées sur le territoire de l'UE à des fournisseurs désignés de services de messagerie financière internationale.

L'avantage conféré par les données TFTP aux États membres, à Europol et à Eurojust est limité par le fait que l'analyse TFTP des paiements transfrontières repose exclusivement sur les messages FIN ("Financial Institution Transfer"), un type de message SWIFT de type servant au transfert d'informations financières d'une institution financière à une autre. Les autres méthodes de paiement ne sont pas prises en considération. Toutefois, le TFTP est le seul mécanisme qui, aux fins de renforcer la sécurité intérieure, permette, dans un délai très court, la cartographie et le profilage de transactions qui sont suspectées d'être liées au terrorisme. En raison d'une meilleure connaissance des clauses de réciprocité figurant dans cet accord, les autorités de l'UE appliquent de plus en plus ce mécanisme, afin de bénéficier de l'échange de données avec les États-Unis. Il convient de noter, dans ce contexte, que toutes les demandes des autorités de l'UE concernant des recherches dans le cadre du TFTP doivent satisfaire aux exigences de l'article 10 de l'accord.

Bien que l'accord ne prévoie pas que les États membres passent par l'intermédiaire d'Europol pour demander une recherche d'informations pertinentes obtenues dans le cadre du TFTP, il serait utile, afin d'améliorer la capacité de réaction de l'UE face au terrorisme et à son financement, que les États membres informent au moins Europol, de manière systématique et en temps utile, de leurs demandes directes présentées au titre de l'article 10. Pour aider les États membres à canaliser les demandes de recherches TFTP, Europol a mis en place un point de contact unique (PCU) et, avec son environnement de fichiers de travail à des fins d'analyse (FTA) et une coopération bien établie avec le département du Trésor, l'agence est bien placée pour traiter les requêtes des États membres de manière efficace.

3.15. Échange d'information sur les casiers judiciaires (ECRIS)

Législation

Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, JO L 93 du 7.4.2009, p. 23. Cette décision-cadre abroge la décision 2005/876/JAI du Conseil du 21 novembre 2005 relative à l'échange d'informations extraites du casier judiciaire, JO L 322 du 9.12.2005, p. 33.

Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil, JO L 151 du 7.6.2019, p. 143.

Principales dispositions

La décision-cadre 2009/315/JAI du Conseil impose à l'État membre de condamnation de transmettre, dès que possible, les condamnations inscrites dans son casier judiciaire à l'État membre ou aux États membres dont cette personne a la nationalité, ainsi que les modifications ou suppressions apportées à cette condamnation. L'État membre de nationalité est tenu de conserver ces informations aux fins de leur retransmission. Toute modification ou suppression effectuée dans l'État membre de condamnation entraîne une modification ou suppression identique dans le casier judiciaire de la personne concernée dans l'État membre ou les États membres dont elle a la nationalité. Des informations sur les condamnations peuvent être demandées à l'État membre de nationalité aux fins d'une procédure pénale ou à toute autre fin qu'une procédure pénale, notamment pour prévenir un danger immédiat et sérieux pour la sécurité publique. Toutefois, l'utilisation d'informations transmises en application de cette décision-cadre à d'autres fins que dans le cadre d'une procédure pénale peut être limitée conformément au droit national de l'État membre requis et de l'État membre requérant afin de ne pas compromettre les chances de réinsertion sociale de la personne condamnée.

La décision 2009/316/JAI du Conseil définit les modalités selon lesquelles un État membre doit transmettre de telles informations. La décision du Conseil établit un cadre pour un système informatisé d'échange d'informations extraites du casier judiciaire. Les autorités centrales de chaque État membre utilisent, en ayant recours à la voie électronique décrite dans la législation, les formulaires de demande et de réponse spéciaux annexés à la décision-cadre.

3.15.1. Échange d'informations sur les casiers judiciaires des ressortissants de pays tiers et des apatrides (ECRIS-TCN)

Législation

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

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

Directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil, JO L 151 du 7.6.2019, p. 143.

Principales dispositions

Le règlement (UE) 2019/816 s'applique au traitement des données d'identification des ressortissants de pays tiers qui ont fait l'objet de condamnations dans les États membres. Par "ressortissant d'un pays tiers", on entend une personne qui n'est pas citoyen de l'Union au sens de l'article 20, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, ou qui est une personne apatride ou dont la nationalité n'est pas connue. Les casiers judiciaires concernant ces personnes sont conservés dans l'État membre de condamnation. L'ECRIS-TCN[104] a pour objectif de permettre de déterminer quels autres États membres détiennent des informations sur le casier judiciaire d'un ressortissant d'un pays tiers. Le cadre de l'ECRIS peut ensuite être utilisé pour demander de telles informations à ces États membres, conformément à la décision-cadre 2009/315/JAI.

Le règlement définit les règles relatives à la création d'un système contenant des données à caractère personnel, dont le développement et la maintenance sont assurés par l'eu-LISA et qui est centralisé au niveau de l'Union, ainsi que les règles relatives à la répartition des responsabilités entre l'État membre et l'organisme responsable du développement et de la maintenance du système centralisé. Il garantit un niveau global approprié de protection et de sécurité des données, ainsi que la protection des droits fondamentaux des personnes concernées.

Eurojust, Europol et le Parquet européen devraient avoir accès au système ECRIS-TCN pour pouvoir identifier les États membres détenant des informations sur le casier judiciaire d'un ressortissant d'un pays tiers aux fins de l'accomplissement de leurs missions statutaires.

3.16. Conservation des données de télécommunications

Législation

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE[105].

---

104 La Commission fixera la date à laquelle l'ECRIS-TCN doit être mis en service, une fois que les conditions énoncées à l'article 35 du règlement (UE) 2019/816 sont remplies.

105 Un arrêt de la Cour de justice de l'Union européenne rendu le 8 avril 2014 a invalidé la directive.

Principales dispositions

La directive s'applique aux fournisseurs de services de communications électroniques. La directive indique que ces fournisseurs doivent conserver les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur, afin de communiquer ces données aux autorités nationales compétentes si elles en font la demande. Aux fins des enquêtes concernant des infractions graves, de leur détection et de leur poursuite, les États membres obligent les fournisseurs de services de communications électroniques ou de réseaux publics de communication à conserver les catégories de données nécessaires pour déterminer:

- la source d'une communication;
- la destination d'une communication;
- la date, l'heure et la durée d'une communication;
- le type de communication;
- le matériel de communication des utilisateurs ou ce qui est censé être leur matériel;
- la localisation du matériel de communication mobile.

Aucune donnée révélant le contenu de la communication ne peut être conservée.

3.17. Directive PNR (dossiers passagers)

Législation

Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

Principales dispositions

La directive établit, au niveau de l'Union, un cadre juridique commun pour le transfert et le traitement des données PNR et prévoit:

b) le transfert, par les transporteurs aériens[106], de données des dossiers des passagers (PNR) de vols extra-UE. Si un État membre décide d'appliquer la directive aux vols intra-UE, toutes les dispositions s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE;

c) le traitement des données PNR, notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

Aux fins du traitement des données PNR, chaque État membre met en place ou désigne une autorité compétente, en tant que son Unité d'informations passagers (UIP). Deux États membres ou plus peuvent mettre en place ou désigner une autorité unique en tant qu'UIP commune.

Les données PNR énumérées à l'annexe I de la directive doivent être transférées aux UIP pour autant qu'elles aient déjà été recueillies par les transporteurs aériens dans le cours normal de leurs activités. Certains transporteurs conservent les informations préalables sur les passagers (données API) en les regroupant avec les données PNR, alors que d'autres ne le font pas. Indépendamment de la manière dont les transporteurs aériens recueillent les données API, ils doivent transférer ces données aux UIP qui les traiteront de la même façon que les données PNR. L'annexe II de la directive contient la liste des infractions graves qui relèvent du champ d'application de la directive.

Le traitement des données PNR sert à évaluer les passagers avant leur arrivée dans un État membre ou leur départ de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, et, le cas échéant, par Europol dans les limites de ses compétences et pour l'accomplissement de ses missions.

---

106 La directive est sans préjudice de la possibilité pour les États membres de prévoir, en vertu de leur droit national, un système de collecte et de traitement des données PNR auprès d'opérateurs économiques autres que les transporteurs, tels que des agences ou des organisateurs de voyages qui fournissent des services liés aux voyages, y compris la réservation de vols, pour lesquels ils recueillent et traitent les données PNR, ou de transporteurs autres que ceux que la présente directive mentionne, sous réserve que ce droit national respecte le droit de l'Union.

Pour réaliser l'évaluation, les UIP peuvent:

a) confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

Au niveau national, les UIP transmettent les données PNR ou le résultat de leur traitement aux autorités répressives nationales compétentes habilitées à poursuivre l'examen du dossier ou à prendre des mesures appropriées aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. S'il est vrai que les UIP constituent le principal canal d'échange d'informations transfrontière, les autorités compétentes peuvent s'adresser directement aux UIP d'un autre État membre dans les cas d'urgence et sous certaines conditions bien définies.

Au niveau de l'Union, les UIP échangent à la fois les données PNR recueillies auprès des transporteurs aériens et le résultat du traitement de ces données entre elles et avec Europol, qui est habilitée, dans les limites de ses compétences et pour l'accomplissement de ses missions, à demander de telles données aux UIP.

Les données PNR doivent être conservées dans une base de données à l'UIP pendant une période de cinq ans suivant leur transfert depuis l'État membre d'arrivée ou de départ du vol. Cependant, toutes les données PNR sont dépersonnalisées après une période de six mois. Cela est effectué par le masquage de tout élément de données qui pourrait servir à identifier directement le passager auquel se rapportent ces données. La liste des données PNR devant être masquées figure dans la directive. Au bout de cinq ans, les données PNR doivent être effacées, sauf si elles ont été transférées à une autorité compétente aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, auquel cas leur conservation est régie par le droit national.

Conformément à la législation de l'UE en matière de protection des données, la directive PNR interdit le traitement de données sensibles telles que l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

3.18. Informations préalables sur les passagers (données API)

Législation

Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers

Principales dispositions

La directive vise à améliorer les contrôles aux frontières et à lutter efficacement contre l'immigration clandestine. Dans ce but, la directive impose aux États membres d'établir l'obligation, pour les transporteurs aériens, de transmettre certaines informations concernant leurs voyageurs avant leur entrée dans l'Union européenne. Ces informations sont désignées sous le nom d'informations préalables sur les passagers (données API). Sous certaines conditions et dans certaines circonstances, les États membres peuvent aussi utiliser les données API à des fins répressives.

Ces informations sont fournies à la demande des autorités chargées du contrôle des personnes aux frontières extérieures de l'UE.

Les transporteurs aériens devraient transmettre les données API par voie électronique ou, en cas d'échec, par tout autre moyen approprié, aux autorités chargées d'effectuer les contrôles au point de passage frontalier par lequel le passager entre dans l'UE. Les données API sont comparées au contenu de bases de données nationales et européennes telles que le Système d'information Schengen (SIS) et le système d'information sur les visas (VIS).

Lorsque des données API correspondent à une entrée dans une base de données (liste de surveillance), un signalement est envoyé à la police des frontières et le passager concerné est ciblé en vue d'un contrôle à son arrivée. Si la correspondance répond à un profil de risque, une cible est créée. Les données API recueillies et transmises devront être effacées par les transporteurs et les autorités dans les vingt-quatre heures qui suivent la transmission ou l'arrivée. Toutefois, les autorités chargées du contrôle aux frontières peuvent conserver le fichier temporaire pendant plus de 24 heures si les données sont nécessaires ultérieurement aux fins de l'exercice des pouvoirs réglementaires des autorités chargées du contrôle aux frontières ou de l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale.

3.19. Infractions en matière de sécurité routière

Législation

Directive (UE) 2015/413 du Parlement européen et du Conseil du 11 mars 2015 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière, JO L 68 du 13.3.2015, p. 9

Principales dispositions

Les États membres s'accordent mutuellement un accès en ligne à leurs données nationales d'immatriculation des véhicules (DIV) en vue de faire appliquer les sanctions prévues pour certaines infractions en matière de sécurité routière commises avec un véhicule immatriculé dans un État membre autre que celui où l'infraction a eu lieu. L'État membre de l'infraction utilise les données obtenues aux fins d'établir qui est personnellement responsable de l'infraction en matière de sécurité routière. L'échange d'informations s'applique:

- aux excès de vitesse;
- au défaut de port de la ceinture de sécurité;
- au franchissement d'un feu rouge;
- à la conduite en état d'ébriété;
- à la conduite sous l'influence de stupéfiants;
- au défaut de port du casque;
- à la circulation sur une voie interdite;
- à l'usage illicite d'un téléphone portable ou de tout autre appareil de communication en conduisant un véhicule.

Au moyen de l'application logicielle spécifique EUCARIS, les États membres autorisent leurs points de contact nationaux (PCN) désignés respectifs à accéder aux DIV, avec le pouvoir de procéder à des consultations automatisées portant sur:

a) les données relatives aux véhicules et

b) les données relatives au propriétaire ou au détenteur du véhicule.

3.20. Système d'entrée/de sortie (EES)

Législation

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.

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

Le règlement (UE) 2017/2226 constitue un développement des dispositions de l'acquis de Schengen.

Le Danemark a fait savoir qu'il a décidé de transposer dans son droit interne les règlements susmentionnés, conformément à l'article 4 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne. Cette décision crée une obligation de droit international entre le Danemark et les autres États membres liés par les mesures en question.

Le Royaume-Uni et l'Irlande ne participent pas à l'acquis de Schengen et ne sont donc pas liés par le règlement ni soumis à son application.

L'Islande, la Norvège, le Liechtenstein et la Suisse sont liés par l'acquis de Schengen au sens des accords et protocoles respectifs concernant l'acquis de Schengen.

En ce qui concerne Chypre, la Bulgarie, la Roumanie et la Croatie, les dispositions du règlement relatives au SIS et au VIS constituent des dispositions fondées sur l'acquis de Schengen ou qui s'y rapportent, au sens des actes d'adhésion respectifs.

Principales dispositions

Le règlement (UE) 2017/2226[107] définit les objectifs de l'EES, les catégories de données à y introduire, les finalités de l'utilisation des données, les critères pour leur introduction et les autorités habilitées à y avoir accès, des règles complémentaires concernant le traitement des données et la protection des données à caractère personnel, ainsi que l'architecture technique de l'EES, les règles concernant son fonctionnement et son utilisation, ainsi que l'interopérabilité avec d'autres systèmes d'information. L'EES a pour objectifs d'améliorer la gestion des frontières extérieures, d'empêcher l'immigration irrégulière et de faciliter la gestion des flux migratoires. À cette fin, l'EES est conçu pour enregistrer et stocker la date, l'heure et le lieu d'entrée et de sortie de certains ressortissants de pays tiers qui franchissent les frontières des États membres auxquelles l'EES est mis en œuvre En outre, les services répressifs des États membres peuvent consulter l'EES aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière[108].

---

107 La Commission fixera la date à laquelle l'EES doit être mis en service, une fois que les conditions énoncées à l'article 66 du règlement (UE) 2017/2226 sont remplies.

108 Par "infraction terroriste", on entend une infraction qui correspond ou est équivalente à l'une des infractions visées dans la directive (UE) 2017/541; Par "infraction pénale grave", on entend une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI relative au mandat d'arrêt européen, si elle est passible, au titre du droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans.

L'EES est composé d'un système central (le système central de l'EES), qui gère une base de données centrale informatisée comprenant des données biométriques et alphanumériques, et d'une interface uniforme nationale dans chaque État membre. Un canal de communication sécurisé relie le système central de l'EES au système central d'information sur les visas (système central du VIS), et une infrastructure de communication sécurisée et cryptée permet de connecter le système central de l'EES à l'interface uniforme nationale. L'interopérabilité est assurée entre l'EES et le VIS au moyen d'un canal de communication direct entre leurs systèmes centraux respectifs, qui permet aux autorités frontalières de consulter le VIS à partir de l'EES et aux autorités chargées des visas de consulter l'EES à partir du VIS.

Le règlement établit des règles strictes d'accès à l'EES. Il fixe aussi le droit des personnes concernées à accéder aux données, à les faire rectifier, compléter, et effacer, ainsi que leur droit à un recours, en particulier le droit à un recours juridictionnel, et prévoit le contrôle des opérations de traitement par des autorités publiques indépendantes.

Le règlement respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne. Sans préjudice de règles plus précises prévues par le règlement (UE) 2017/2226 en ce qui concerne le traitement de données à caractère personnel, le règlement (UE) 2016/679[109] (règlement général sur la protection des données) s'applique au traitement de données à caractère personnel réalisé en application du règlement (UE) 2017/2226, sauf si ce traitement est effectué par les autorités répressives désignées ou par les points d'accès centraux des États membres, auxquels cas la directive (UE) 2016/680[110] (directive "police" relative à la protection des données) s'applique.

---

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

110 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2019 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

3.21. Système européen d'information et d'autorisation concernant les voyages (ETIAS)

Législation

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.

Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), JO L 236 du 19.9.2018, p. 72.

Le règlement (UE) 2018/1240[111] précise les objectifs d'ETIAS, définit son architecture technique et organisationnelle, fixe les règles d'exploitation du système et d'utilisation des données introduites par les demandeurs ainsi que les règles relatives à la délivrance ou au refus des autorisations de voyage, arrête les finalités du traitement des données, détermine les autorités habilitées à accéder aux données et garantit la protection des données à caractère personnel.

Le règlement constitue un développement des dispositions de l'acquis de Schengen. Le Royaume-Uni et l'Irlande ne participent pas à l'acquis de Schengen et ne sont donc pas liés par le règlement ni soumis à son application. L'Islande, la Norvège, le Liechtenstein et la Suisse sont liés par l'acquis de Schengen au sens des accords et protocoles respectifs concernant l'acquis de Schengen.

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) nº 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, JO L 135 du 22.5.2019, p. 27.

---

111 La Commission fixera la date à laquelle l'ETIAS doit être mis en service, une fois que les conditions énoncées à l'article 88 du règlement (UE) 2018/1240 sont remplies.

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, JO L 135 du 22.5.2019, p. 85.

Principales dispositions

L'ETIAS fournit une autorisation de voyage, qui est par nature différente d'un visa mais constitue une condition d'entrée et de séjour dans l'espace Schengen, et qui indique que le demandeur d'une autorisation de voyage ne présente pas un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé dans l'Union.

L'ETIAS est composé:

- d'un système d'information à grande échelle, le système d'information ETIAS, dont la conception, le développement et la gestion technique sont assurés par l'eu-LISA;
- de l'unité centrale ETIAS, qui fait partie de l'Agence européenne de garde-frontières et de garde-côtes;
- des unités nationales ETIAS, qui sont chargées d'examiner les demandes et de décider de délivrer, de refuser, d'annuler ou de révoquer les autorisations de voyage. À cette fin, les unités nationales devraient coopérer entre elles ainsi qu'avec Europol aux fins de l'évaluation des demandes.

L'accès aux données à caractère personnel figurant dans l'ETIAS devrait être limité au personnel strictement autorisé et ne devrait en aucun cas être utilisé pour prendre des décisions fondées sur l'une ou l'autre forme de discrimination. En ce qui concerne les autorités répressives désignées par les États membres, le traitement de données à caractère personnel stockées dans le système central ETIAS ne devrait avoir lieu que dans des cas spécifiques et pour autant que cela soit nécessaire aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux fins des enquêtes en la matière. Les autorités désignées et Europol ne devraient demander l'accès à l'ETIAS que lorsqu'elles ont des motifs raisonnables de penser que cet accès leur permettra d'obtenir des informations qui les aideront à prévenir ou à détecter une infraction terroriste ou une autre infraction pénale grave, ou à enquêter en la matière.

Le règlement respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne. Pour ce qui est du traitement de données à caractère personnel, des garanties appropriées visent par conséquent à limiter l'ingérence vis-à-vis du droit à la protection de la vie privée et du droit à la protection des données à caractère personnel à ce qui est nécessaire et proportionné dans une société démocratique.

Le règlement (UE) 2016/679[112] (règlement général sur la protection des données) s'applique au traitement de données à caractère personnel réalisé en application du règlement (UE) 2018/1240, sauf si ce traitement est effectué par les autorités répressives désignées ou par les points d'accès centraux des États membres, auxquels cas la directive (UE) 2016/680[113] (directive "police" relative à la protection des données) s'applique.

3.22. Législation relative à l'interopérabilité

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) nº 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, JO L 135 du 22.5.2019, p. 27.

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, JO L 135 du 22.5.2019, p. 85.

---

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

113 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2019 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

Principales dispositions

Le règlement (UE) 2019/817 et le règlement (UE) 2019/818 constituent le train de mesures sur l'interopérabilité et portent principalement sur les données à caractère personnel qui sont conservées dans les systèmes d'information centralisés au niveau de l'UE. Ces règlements visent à améliorer l'architecture de la gestion des données de l'Union appliquée à la gestion des frontières et à la sécurité. Par conséquent, le cadre défini par le train de mesures sur l'interopérabilité s'applique au traitement des données à caractère personnel aussi bien dans le domaine des frontières et des visas qu'en matière de coopération policière et judiciaire, d'asile et de migration. L'interopérabilité entre ces systèmes d'information sous-jacents devrait leur permettre de se compléter afin de mieux réaliser leurs objectifs respectifs.

Les règlements adaptent également les procédures et les conditions d'accès des autorités désignées et d'Europol à l'EES, au VIS, à l'ETIAS et à Eurodac aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière.

Les éléments d'interopérabilité technique englobent l'EES (voir point 3.19), le VIS (voir point 3.8), l'ETIAS (voir point 3.20), Eurodac (voir point 3.9), le SIS (voir point 3.3) et l'ECRIS-TCN (voir point 3.14.1). Les éléments d'interopérabilité[114] sont les suivants:

- un portail de recherche européen, qui consiste en un guichet unique ou un "courtier de messages" permettant d'interroger en parallèle les systèmes d'information de l'UE susmentionnés, les données d'Europol et les bases de données d'Interpol. Les requêtes sont limitées aux données relatives à des personnes ou à des documents de voyage;

- un service partagé d'établissement de correspondances biométriques (BMS partagé), dont l'objectif principal est de faciliter l'identification d'une personne enregistrée dans plusieurs bases de données, en utilisant un élément technologique unique pour faire correspondre les données biométriques de cette personne contenues dans différents systèmes. Les modèles biométriques utilisés pour les systèmes automatisés d'identification par empreintes digitales devraient être regroupés et stockés dans le BMS à un seul endroit;

[114] La Commission fixera la date à partir de laquelle s'appliqueront les dispositions des règlements relatives à l'ESP, au BMS partagé, au CIR et au MID.

- un répertoire commun de données d'identité (CIR), conçu comme un réservoir partagé pour les données d'identité, les documents de voyage et les données biométriques des personnes enregistrées dans l'EES, le VIS, l'ETIAS, Eurodac et l'ECRIS-TCN. Ces données peuvent concerner la même personne, mais sous des identités différentes ou incomplètes. La comparaison et la mise en correspondance automatisées des données devraient permettre d'améliorer la précision de l'identification. Les autorités répressives désignées peuvent réaliser des contrôles d'identité à l'aide du CIR afin de pouvoir identifier une personne;

- un détecteur d'identités multiples (MID), qui soutient le fonctionnement du CIR.

Les nouvelles opérations de traitement de données prévues par les règlements constituent une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. Étant donné que la mise en œuvre effective des systèmes d'information de l'UE dépend de l'identification correcte de la personne concernée, une telle atteinte correspond aux objectifs pour lesquels chacun de ces systèmes a été créé, à savoir la gestion efficace des frontières de l'Union, la sécurité intérieure de l'Union et la mise en œuvre efficace des politiques de l'Union en matière d'asile et de visas.

Le règlement (UE) 2016/679 s'applique au traitement de données à caractère personnel effectué à des fins d'interopérabilité, à moins que ce traitement ne soit effectué par les autorités répressives désignées ou par les points d'accès centraux des États membres à des fins de prévention et de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, auquel cas la directive (UE) 2016/680 (voir point 3.1) s'applique.

Les autorités de contrôle visées dans le règlement (UE) 2016/679 ou la directive (UE) 2016/680 devraient contrôler la licéité du traitement de données à caractère personnel par les États membres. Le Contrôleur européen de la protection des données devrait contrôler les activités des institutions et organes de l'Union concernant le traitement de données à caractère personnel.