Nom	Description
Un fichier est « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.* » Article 4, 6) du Règlement général sur la protection des données *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679* « *Un fichier est un traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés.* » La CNIL *https://www.cnil.fr/fr/glossaire*	
AGDREF 2 *(Application de Gestion des Dossiers des Ressortissants Etrangers en France)* ***– page 4***	Ce fichier concerne toutes les personnes étrangères ayant entrepris des démarches relatives au séjour en France. Il permet d'identifier les étrangers présents sur le territoire. Il poursuit un objectif de lutte contre la fraude et les fausses identités déclinées sur de faux documents.
DNA *(Dispositif National d'Accueil des demandes d'asile)* ***– page 7***	Ce fichier contient des données relatives aux demandeurs d'asile en France, dans le but de gérer l'accueil national des demandeurs d'asile, notamment les lieux d'hébergement et les conditions matérielles d'accueil.
FAED *(Fichier Automatisé des Empreintes Digitales)* ***– page 9***	Cette base de données contient les empreintes digitales des personnes mises en cause dans une procédure criminelle ou délictuelle afin de les identifier, mais également celles des personnes retenues pour vérification de leur identité.
Fichier S *(Atteinte à la sûreté de l'Etat)* ***– page 11***	Ce fichier contient des informations concernant des personnes faisant l'objet de recherches pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'Etat, afin de faciliter les recherches ou la surveillance de celles-ci.
FNAEG *(Fichier National Automatisé des Empreintes Génétiques)* ***– page 13***	Cette base de données contient les empreintes génétiques, c'est-à-dire les séquences d'ADN de personnes ayant commis des infractions afin de faciliter leur identification et leur recherche. Il est également utilisé pour vérifier l'identité des personnes retenues à cette fin.
FPR *(Fichier des Personnes Recherchées)* ***– page 15***	Ce fichier recense toutes les personnes recherchées pour des motifs judiciaires, administratifs ou d'ordre public, afin de faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives. Il est divisé en 21 sous-fichiers en fonction du fondement juridique de la recherche. Il est consulté avant la délivrance d'un permis de séjour et ses données sont également reversées dans le fichier SIS II.
GESTEL *(Gestion de l'Eloignement)* ***– page 17***	Ce fichier vise à améliorer le suivi et l'exécution des procédures d'éloignement en enregistrant un ensemble de données relatives aux personnes faisant l'objet d'une mesure d'éloignement.
GIPI *(Gestion Informatisée des Procédures d'Immigration)* ***– page 19***	Il recense un ensemble de données relatives aux personnes non-admises sur le territoire Schengen. Il permet de faciliter la gestion des procédures de non-admission des étrangers qui ne remplissent pas les conditions d'entrée dans l'espace Schengen entre les Etats signataires de l'accord de Schengen, ainsi que le traitement et le suivi des amendes infligées aux entreprises de transports.
INEREC *(Instruction et Recours)* ***– page 21***	Cette base de données contient les données relatives aux demandes d'asile en cours. Elle a pour but de permettre une meilleure gestion par l'OFPRA des demandes par l'échange d'informations avec les préfectures et le ministère de l'intérieur.

OSCAR *(Outil de Statistique et de Contrôle de l'Aide au Retour)* ***– page 23***	Ce fichier contient les données relatives aux personnes ayant bénéficié de l'aide volontaire au retour accordée par l'OFII. Il permet notamment de déceler si une demande d'aide volontaire au retour a été présentée par une personne en ayant déjà bénéficié, le cas échéant sous une autre identité.
RMV2 *(Réseau Mondial Visa)* ***– page 25***	Ce fichier est consulté à chaque instruction de dossier de demande de visa, dans lequel sont enregistrées toutes les demandes de visas faites dans les consulats français de par le monde. Cette consultation permet de savoir si le demandeur est signalé dans une des autres bases de données auxquelles donne accès le réseau.
SILCF *(Système Informatisé concourant au dispositif de Lutte Contre les Fraudes)* ***– page 27***	Ce traitement est mis en œuvre par la direction générale des douanes et droits indirects, afin d'aider à la bonne exécution des missions de recherche, de constatation, de poursuite et de répression des fraudes.
TAJ *(Traitement d'Antécédents Judiciaires)* ***– page 30***	Ce fichier contient les données relatives aux personnes interpellées pour des antécédents judiciaires par la police, la gendarmerie nationale et les agents des douanes judiciaires. Il est utilisé dans le cadre d'enquêtes judiciaires (recherche des auteurs d'infractions) et dans le cadre d'enquêtes administratives (par exemple : enquêtes préalables à certains emplois publics ou sensibles).
TES *(Titre Electronique Sécurisé)* ***– page 33***	Ce fichier recense des données concernant les demandeurs d'un titre d'identité ou les titulaires en demandant le renouvellement. Il est un outil de contrôle d'éventuelles falsifications de documents d'identité.
VISABIO *(Visa Biométrique)* ***– page 35***	Ce fichier vise à améliorer les conditions de délivrance des visas (vérification de l'identité et de l'authenticité des visas) et faciliter les vérifications d'identité sur le territoire français.
EURODAC *(EU Biometric Data Base)* ***– page 37***	Ce fichier contient les empreintes digitales des demandeurs d'asile et des étrangers entrés irrégulièrement ou en situation irrégulière sur le territoire d'un Etat. Il est utilisé par les Etats-membres pour mettre en œuvre la Convention Dublin sur le traitement des demandes d'asile.
SIS II *(Système d'Information Schengen)* ***– page 40***	Ce fichier est commun à l'ensemble des États membres de l'espace Schengen et permet à chaque Etat d'émettre et de consulter des signalements concernant notamment des personnes recherchées ou disparues, sous surveillance policière ou non ressortissantes d'un État membre de l'espace Schengen auxquelles l'entrée sur le territoire Schengen est interdite. Il a peu à peu glissé vers un système d'enquête policière à l'échelle européenne intégrant des données biométriques.
VIS *(Visa Information System)* ***– page 43***	Ce fichier contient les données relatives aux demandes de visas de court séjour. Il permet un échange d'informations entre les Etats membres pour répondre à divers objectifs notamment lutter contre la fraude ou faciliter l'application du Règlement Dublin III, mais également lutter contre les demandes de visas multiples au sein de l'espace Schengen.
API-PNR *(Advance Passenger Information - Personal Name Record)* ***– page 46***	Les données de réservation et d'enregistrement des passagers aériens sont contenues dans ce fichier. Ces données sont rapprochées avec d'autres fichiers de police judiciaire et administrative tel que le FPR, le SIS II ou le SILCF par leur enregistrement dans le système API-PNR.
EUROPOL *(European Police Office)* ***– page 48***	Europol est une organisation intergouvernementale destinée à faciliter la coopération policière européenne. Elle permet de faciliter l'échange d'informations entre les Etats membres, concernant des personnes suspectées ou accusées d'infraction pénale à l'échelle européenne.
INTERPOL *(Organisation Internationale de Police criminelle)* ***– page 50***	Interpol est une organisation de coopération policière internationale ayant pour objectif de lutter contre la criminalité. A cette fin, elle met en œuvre un traitement de données alimenté par des signalements appelés notices émis par les pays membres.

Définitions	***Interconnexion*** : le partage de données contenues dans plusieurs fichiers, c'est-à-dire « l'objet même d'un traitement qui permet d'accéder à, d'exploiter, et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu. » *Définition du Conseil d'Etat, arrêt n°317182 du 19 juillet 2010* *https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000022512947* ***Interopérabilité*** : la capacité des systèmes d'information à échanger des données et à permettre le partage d'informations. Il y a 4 dimensions en matière d'interopérabilité : ⇨ une interface de recherche unique permettant d'interroger simultanément plusieurs systèmes d'information et de produire des résultats combinés sur un seul écran. ⇨ l'interconnexion des systèmes d'information, qui permet aux données enregistrées dans un système d'être automatiquement consultées par un autre système. ⇨ la mise en place d'un service partagé de mise en correspondance de données biométriques à l'appui de divers systèmes d'information. ⇨ un répertoire commun de données pour différents systèmes d'information (module central). *Définition de la Commission européenne, Communication au Parlement européen et au Conseil, Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité COM/2016/0205 final* *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM%3A2016%3A205%3AFIN*
	Droit d'accès et de communication des données : ce droit est prévu à l'*article 39 de la loi n°78-17 du 6 janvier 1978 (dernière modification par la loi n°2018-493 du 20 juin 2018)* et permet à toute personne d'interroger le responsable d'un traitement de données à caractère personnel, afin de savoir s'il fait l'objet d'un traitement de données personnelles et de connaître les finalités du traitement. Tout individu a aussi le droit de recevoir les informations nécessaires pour connaître et contester la logique qui sous-tend le traitement automatisé s'il en résulte une décision le concernant. ***Droit de rectification ou d'effacement des données*** : ce droit est prévu à *l'article 40 de la loi n°78-17 du 6 janvier 1978 (dernière modification par la loi n°2018-493 du 20 juin 2018)* et permet à toute personne concernée par une collecte de données d'exiger du responsable de traitement que ses données à caractère personnel soient rectifiées, complétées, mises à jour, verrouillées ou effacées lorsqu'elles sont inexactes, incomplètes, équivoques, périmées ou lorsque leur collecte, leur utilisation, leur communication ou leur conservation sont en réalité interdites. ***Droit d'opposition*** : ce droit est prévu par *l'article 38 de la loi n°78-17 du 6 janvier 1978 (dernière modification par la loi n°2018-493 du 20 juin 2018)* et permet à toute personne de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Cependant, ce droit ne s'applique pas lorsque le traitement répond à une obligation légale ou lorsque qu'il a été expressément écarté par l'acte autorisant le traitement.

Abréviations	**CESEDA** : Code de l'Entrée et du Séjour des Etrangers et du Droit d'Asile **CNIL** : Commission Nationale de l'Informatique et des Libertés **OFII** : Office Français de l'Immigration et de l'Intégration **OFPRA** : Office Français de Protection des Réfugiés et Apatrides **PAF** : Police aux frontières

Nom du fichier	**AGDREF 2**
Sens de l'acronyme	Application de Gestion des Dossiers des Ressortissants Etrangers en France *Les anciens fichiers AGDREF et ELOI ont fusionné au sein du fichier AGDREF 2*
Objectif explicite	L'AGDREF 2 a pour finalités de : • **garantir le droit au séjour des ressortissants étrangers en situation régulière** • **lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers** A cet effet, il a vocation à : • permettre aux services centraux et locaux du ministère de l'intérieur d'assurer l'instruction des demandes et la fabrication des titres de séjour / de voyage / documents de circulation et la gestion des dossiers des ressortissants étrangers • mieux coordonner l'action des services chargés de mettre en œuvre des procédures intéressant les ressortissants étrangers • améliorer les conditions de vérification de l'authenticité des titres de séjour et de l'identité des étrangers en situation irrégulière • permettre la gestion des différentes étapes de la procédure applicable aux mesures d'éloignement • établir des statistiques en matière de séjour et d'éloignement des ressortissants étrangers • aider à déterminer et de permettre de vérifier l'identité d'un étranger qui présente une demande d'asile en Guadeloupe, en Guyane, en Martinique, à Mayotte, à La Réunion, à Saint-Martin, à Saint-Barthélemy et à Saint-Pierre-et-Miquelon • aider à déterminer et de permettre de vérifier l'identité d'un étranger qui se déclare mineur et privé temporairement ou définitivement de la protection de sa famille • permettre au ressortissant étranger titulaire d'un visa de long séjour mentionné aux 4° à 14° de l'article R. 311-3 du CESEDA de procéder par voie électronique aux formalités prévues au même article et permettant de conférer au titulaire de ce visa les droits attachés à une carte de séjour *Article R. 611-1 du CESEDA*
Objectif implicite/ Remarques	Lutter contre la fraude par le contrôle des faux documents. Meryem Merzouki chercheuse au CNRS en informatique, remarque qu'il y a un glissement progressif des finalités initiales de ce fichier. En effet, le fichier est ouvert d'accès à la police, à la gendarmerie et aux services de renseignement de la défense à partir de 2007 suite à un décret pris en application de la loi de lutte contre le terrorisme de janvier 2006. Les finalités du système de fichage n'ayant pas été modifiées, il apparaît selon cette auteure qu'il y ait eu un détournement des finalités initiales du fichier dans une perspective sécuritaire. *Remarque* : Lorsque le fichier ELOI a été supprimé, une partie des données relatives à l'éloignement a été intégrée au fichier AGDREF 2 (décret n°2011-638 du 8 juin 2011). Le décret n°2019-81 du 6 février 2019 a créé un nouveau fichier spécifique à la gestion des mesures d'éloignement, le GESTEL (voir ci-après). Dans sa *délibération n°2018-162 du 17 mai 2018* relative à la création de ce fichier, la CNIL a estimé que certaines données figuraient également dans le traitement AGDREF 2 et devaient en être supprimées dès lors qu'elles étaient intégrées dans le premier fichier. Ces données concernent l'éloignement (ex : escortes des transferts, réservation du moyen de transport sollicité...). En effet, elles n'ont une utilité qu'en matière de gestion opérationnelle, matérielle et logistique des mesures d'éloignement, soit la finalité du traitement GESTEL. La CNIL estime « que l'absence de finalité de gestion de la phase d'exécution concrète des mesures d'éloignement de AGDREF 2 et la création du traitement GESTEL, qui vise précisément une telle gestion, impliquent que de telles données soient retirées du traitement AGDREF 2 ». L'annexe 6-4 du CESEDA (développée ci-dessous), n'a cependant pas été modifiée et les données relatives à l'éloignement sont toujours enregistrées dans l'AGDREF 2.

Contenu des données	• Les fichiers départementaux gérés par les préfectures et un fichier national géré par le ministère de l'intérieur • Les images numérisées de la photographie et des empreintes digitales des dix doigts des étrangers (*article R. 611-2 du CESEDA*) : - demandeurs ou titulaires d'un titre de séjour, d'un titre de voyage d'une durée de validité supérieure à un an ou de la carte de frontalier - en situation irrégulière - faisant l'objet d'une mesure d'éloignement - demandeurs d'asile en Guadeloupe, Guyane, Martinique, Mayotte, La Réunion, Saint-Martin, Saint-Barthélemy, Saint-Pierre-et-Miquelon • Etat civil du demandeur • Sa nationalité • Sa situation de famille • Son adresse • Les conditions de son entrée en France (entrée régulière / irrégulière, regroupement familial...) • Sa profession • Sa situation administrative (carte de séjour / carte de résident / demande de naturalisation / demande d'asile / refus de séjour / reconduite à la frontière / visa de sortie-retour / contentieux) • Si la personne est soumise à une procédure d'éloignement : données relatives à la mesure d'éloignement (nature de la mesure, préfecture en charge de l'exécution de la mesure...), données relatives aux procédures juridictionnelles mises en œuvre dans le cadre de l'éloignement (soustraction à l'exécution de la mesure, recours contentieux...), données relatives à la rétention administrative, données relatives à la gestion administrative et opérationnelle de l'éloignement (escortes des transferts, réservation au moyen de transport international...)... ↳ *Liste exhaustive des données à l'annexe 6-4 du CESEDA* : *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=36596416B965B7DF000C12ED46971206.tplgfr26s_3?idSectionTA=LEGISCTA000024151514&cidTexte=LEGITEXT000006070158&dateTexte=20190305* ↳ Un numéro d'identification national permanent est attribué à chaque ressortissant étranger figurant dans le traitement.
Critères d'inscription dans ce fichier	Etre un ressortissant étranger et avoir entrepris des démarches administratives de droit au séjour en France ou depuis l'étranger
Date de création	8 juin 2011
Autorité(s) compétente(s)	Le ministère de l'intérieur - Direction générale des étrangers en France
Qui a accès à ce fichier ?	• Les services du ministère de l'intérieur compétents pour l'application de la réglementation relative aux étrangers • L'OFPRA • Les services de préfecture et de sous-préfecture compétents pour l'application de la réglementation relative aux étrangers • Les magistrats de l'ordre judiciaire • Les agents de représentation diplomatique et consulaire qui instruisent les demandes de visa • Les services de police nationale et de gendarmerie nationale • Les inspecteurs du travail • Les services chargés des missions de prévention des actes terroristes • L'INSEE • L'INED • L'Organisme de sécurité sociale obligatoire • Pôle emploi • Les agents chargés de la mise en œuvre de la protection de l'enfance

Durée de conservation des données	• Tout dossier n'ayant fait l'objet d'aucune mise à jour dans un délai de cinq ans à compter de l'enregistrement des premières données est effacé, sauf dans les cas listés aux *1° à 4° l'article R. 611-7-1 du CESEDA* : *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=D9F65FA8C9A8ABE25569DF52B58E08CE.tplgfr34s_2?idSectionTA=LEGISCTA000024149389&cidTexte=LEGITEXT000006070158&dateTexte=20190225* • Les données relatives aux personnes ayant acquis la nationalité française sont effacées au terme d'un délai d'un an à compter du décret de naturalisation ou au terme d'un délai de six mois après la date d'enregistrement en cas de déclaration de nationalité • Les données relatives à l'éloignement sont, en cas de délivrance d'une carte de séjour, effacées sans délai dès la délivrance de la carte de séjour • Les nom, prénom et adresse de la personne qui héberge un étranger assigné à résidence sont effacés sans délai après la fin de l'assignation à résidence
Interconnexion avec d'autres fichiers ?	• Aucune interconnexion n'est possible avec d'autres fichiers • A l'exception du fichier « IMMI 2 » de l'OFII, qui est lié à la visite médicale obligatoire des étrangers et à l'attribution de visas de long séjour valant titre de séjour • Le fichier des personnes recherchées (FPR) est automatiquement consulté avant toute délivrance d'autorisation de séjour
Quelle échelle ?	• Fichiers départementaux gérés par les préfectures • Fichier national géré par le ministère chargé de l'immigration Le fichier national central est alimenté par les fichiers départementaux gérés par les préfectures. Le groupe gestionnaire de ce fichier est le « Thales security system ».
Lois qui régissent ce fichier	- CESEDA, article R. 611-1 à R. 611-7-4 (dernière modification du décret n°2019-57 du 30 janvier 2019). *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=D9F65FA8C9A8ABE25569DF52B58E08CE.tplgfr34s_2?idSectionTA=LEGISCTA000024151374&cidTexte=LEGITEXT000006070158&dateTexte=20190225* - CESEDA, Annexe 6-4 (dernière modification du décret n°2019-57 du 30 janvier 2019). *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=36596416B965B7DF000C12ED46971206.tplgfr26s_3?idSectionTA=LEGISCTA000024151514&cidTexte=LEGITEXT000006070158&dateTexte=20190305* - Décret n°2016-1457 du 28 octobre 2016 pris pour l'application de la loi n° 2016-274 du 7 mars 2016 relative au droit des étrangers en France et portant diverses dispositions relatives à la lutte contre l'immigration irrégulière. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D9F65FA8C9A8ABE25569DF52B58E08CE.tplgfr34s_2?cidTexte=JORFTEXT000033318061&dateTexte=20161031* - Décret n° 2013-1082 du 29 novembre 2013 portant modification du code de l'entrée et du séjour des étrangers et du droit d'asile (partie réglementaire) et du décret n° 2011-638 du 8 juin 2011 relatif à l'application de gestion des dossiers des ressortissants étrangers en France et aux titres de séjour et aux titres de voyage des étrangers. *https://www.legifrance.gouv.fr/eli/decret/2013/11/29/INTV1315405D/jo/texte* - Décret n° 2013-147 du 18 février 2013 relatif à l'application de gestion des dossiers de ressortissants étrangers en France et au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027088465&categorieLien=id* - Décret n° 2011-638 du 8 juin 2011 relatif à l'application de gestion des dossiers des ressortissants étrangers en France et aux titres de séjour et aux titres de voyage des étrangers. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024147941&categorieLien=id* - Délibération n° 91-033 du 7 mai 1991 de la CNIL concernant la création du fichier ADGREF. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652649*
Comment obtenir communication et rectification des données ?	• S'agissant du titre de séjour et du titre de voyage : auprès de l'autorité de délivrance du titre de séjour • S'agissant des mesures d'éloignement : auprès du préfet en charge de la gestion du dossier d'éloignement
Sources	- M. Marzouki, « Le fichier des étrangers », Mouvements, n°62, 2010. *http://histoirecoloniale.net/les-fichiers-des-etrangers.html* - D. Lochak, « Des fichiers pour gérer, contrôler et surveiller les étrangers », Plein droit, n°71, 2006. *https://www.cairn.info/revue-plein-droit-2006-4-page-24.htm* - CNIL, « ADGREF : Application de gestion de dossiers des ressortissants étrangers en France ». *https://www.cnil.fr/fr/agdref-application-de-gestion-des-dossiers-des-ressortissants-etrangers-en-France* - Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ».

Nom du fichier	**DNA**
Sens de l'acronyme	Dispositif National d'Accueil des demandeurs d'asile
Objectif explicite	Ce traitement a pour finalités de permettre à l'OFII : • De coordonner la gestion des lieux d'hébergement dédiés aux demandeurs d'asile et de recenser les offres d'hébergement existantes et disponibles • De procurer les conditions matérielles d'accueil réservées aux demandeurs d'asile, en évaluant leurs besoins ainsi que leur vulnérabilité • D'assurer l'orientation des demandeurs d'asile et leur répartition dans les centres d'hébergement dédiés, conformément aux schémas national et régionaux d'accueil des demandeurs d'asile et en fonction des caractéristiques de l'offre et du profil des demandeurs • De vérifier l'acceptation des conditions matérielles d'accueil, et notamment de l'offre d'hébergement, par les demandeurs d'asile • D'allouer l'allocation aux demandeurs d'asile éligibles, aux personnes titulaires d'un titre de séjour remis sur le fondement de l'article L. 316-1 ainsi qu'aux bénéficiaires de la protection temporaire, dans les conditions prévues par l'article L. 744-10 • D'assurer l'accompagnement social et administratif des demandeurs d'asile • De gérer les entrées et les sorties des lieux d'hébergement visés à l'article L. 349-3 du code de l'action sociale et des familles • D'informer le demandeur d'asile sur les dispositifs d'intégration, de retour et de réinsertion que gère l'Office. *Article R. 744-45 du CESEDA*
Objectif implicite/ Remarques	Dans son article « Fichage des demandeurs d'asile. Le logiciel dn@ corrigé par la CNIL » du 15 février 2009, Gérard Sadik, coordinateur national asile de La Cimade, remarque que le fichier DNA intègre des informations comprises dans le fichier ADGREF et INEREC alors que ces rapprochements sont pourtant interdits. Cela traduit un contrôle accru des demandeurs d'asile.
Contenu des données	• L'identité • Le lieu de logement • Les ressources personnelles • Les données relatives à la demande d'asile • Les numéros AGDREF, INEREC et éventuellement SKIPPER correspondant au recours formé devant la Cour nationale du droit d'asile du demandeur d'asile • L'avis du médecin de l'OFII prévu à l'article R. 744-14 relatif à l'adaptation des conditions d'accueil • Les coordonnées bancaires • Les dates de signature du contrat d'intégration républicaine et de convocation à cette fin • La date de transfert vers l'État membre responsable ou du constat de fuite, pour les demandeurs relevant de la procédure Dublin III ↳ *Liste exhaustive à l'annexe 7-2 du CESEDA* : *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=29C30C618766D5DBC9015914502C89FC.tplgfr22s_2?idSectionTA=LEGISCTA000034527208&cidTexte=LEGITEXT000006070158&dateTexte=20190225*
Critères d'inscription dans ce fichier	Etre demandeur d'asile
Date de création	Décision du directeur général de l'OFII n°2009-202 du 29 mai 2009
Autorité(s) compétente(s)	L'OFPRA, l'OFII, le SIAO (Service intégré d'accueil et d'orientation)

Qui a accès à ce fichier ?	• Les agents de l'OFII chargés de la gestion du dispositif national d'accueil, affectés à la direction de l'asile, à l'agence comptable et aux bureaux chargés de l'asile au sein de ses directions territoriales, individuellement désignés et spécialement habilités à cette fin par le directeur général de l'OFII • Les agents chargés de l'accueil des demandeurs d'asile relevant des services centraux et déconcentrés des ministères de l'intérieur et des affaires sociales, individuellement désignés et spécialement habilités par le directeur général de l'OFII • Les agents des structures d'hébergement destinés à recevoir des demandeurs d'asile (CADA, HUDA...) et les personnes bénéficiant d'une protection internationale (centres provisoires d'hébergement) *Article R. 744-47 du CESEDA*
Durée de conservation des données	Les données et informations enregistrées sont conservées pour une durée maximale de deux ans à compter de la notification de la décision définitive sur la demande d'asile. *Article R. 744-49 du CESEDA*
Interconnexion avec d'autres fichiers ?	• Les données du traitement ne font pas l'objet d'une cession ni d'une interconnexion, mise en relation ou rapprochement avec un autre traitement. • Par exception, les données d'état civil du demandeur d'asile et les données relatives à la situation administrative du demandeur d'asile mentionnées aux I et II de l'annexe 7-2 du CESEDA sont transmises à l'OFII par l'intermédiaire de l'application AGDREF 2. Ces mêmes données sont transmises aux personnels de santé de l'OFII par l'intermédiaire du traitement DNA quand le médecin de l'office est saisi pour émettre un avis dans les conditions fixées par l'article R. 744-14 du CESEDA. *Article R. 744-50 du CESEDA*
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Code de l'entrée et du séjour des étrangers et du droit d'asile, articles R. 744-45 à R. 744-52. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=624D60BD44BF5F94A87365749D87F66C.tplgfr22s_2?idSectionTA=LEGISCTA000034526822&cidTexte=LEGITEXT000006070158&dateTexte=20190225* - Décret n°2017-665 du 27 avril 2017 relatif au traitement de données à caractère personnel de gestion des conditions matérielles d'accueil des demandeurs d'asile, dénommé DNA. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034512966&categorieLien=id* - Délibération n° 2016-393 du 15 décembre 2016 portant avis de la Commission nationale de l'informatique et des libertés. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034513454*
Comment obtenir communication et rectification des données ?	Les droits d'accès et de rectification s'exercent auprès du directeur général de l'OFII *Article R. 744-52 du CESEDA*
Sources	- G. Sadik, « Fichage des demandeurs d'asile. Le logiciel dn@ corrigé par la CNIL », 15 février 2009. *http://combatsdroitshomme.blog.lemonde.fr/2009/02/15/le-logiciel-dn-corrige-par-la-cnil-par-gerard-sadik/* - Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ».

Nom du fichier	**FAED**
Sens de l'acronyme	Fichier Automatisé des Empreintes Digitales.
Objectif explicite	• Il sert à la recherche et l'identification des auteurs de crimes et de délits et à la poursuite / instruction / jugement des affaires criminelles et délictuelles dont l'autorité judiciaire est saisie. ⇨ Il permet de s'assurer de la véritable identité des personnes mises en cause dans une procédure pénale ou condamnées à une peine privative de liberté, afin d'éviter les erreurs judiciaires, de détecter les fausses identités et établir les cas de récidive. • Faciliter la recherche de personnes disparues et l'identification de personnes décédées ou grièvement blessées. • Il permet de vérifier l'identité de personnes retenues aux fins de vérification de leur identité *(article 78-3 du code de procédure pénale et L. 611-4 du CESEDA*).
Objectif implicite/ Remarques	Ce fichier comprend un grand nombre d'informations, pas seulement des données nationales mais aussi des données transmises par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers. *Remarque* : La CEDH a condamné la France en 2013 pour ce fichier au motif que « *la conservation des empreintes digitales par ce fichier s'analyse en une atteinte disproportionnée, ne peut passer pour nécessaire dans une société démocratique, et ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu* » (*CEDH, 5e Sect., Affaire M.K. c. France, 18 juillet 2013, Req. n°19522/09*). Pourtant, ce fichier n'a été corrigé à la marge que deux ans après l'arrêt de la CEDH.
Contenu des données	En plus des empreintes digitales, d'autres données sont enregistrées : • nom, prénom, date et lieu de naissance, éléments de filiation, sexe • le service ayant procédé à la signalisation • la date et le lieu d'établissement de la fiche signalétique • la nature de l'affaire et la référence de la procédure • les clichés anthropométriques • si les empreintes sont transmises par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers, sont enregistrées l'origine de l'information et la date de son enregistrement dans le traitement
Critères d'inscription dans ce fichier	• Les personnes mises en cause lors d'une procédure criminelle ou délictuelle (enregistrements des traces d'empreintes, des empreintes digitales etc.) • Les personnes décédées (empreintes digitales et palmaires) • Les personnes grièvement blessées et dont l'identité n'a pu être établie
Date de création	8 avril 1987
Autorité(s) compétente(s)	La direction centrale de la police judiciaire du ministère de l'intérieur, sous le contrôle d'un magistrat de l'ordre judiciaire
Qui a accès à ce fichier ?	Les fonctionnaires et militaires habilités des services d'identité judicaire de la police nationale, du service central de renseignement criminel de la gendarmerie nationale, ainsi que des unités de recherches de la gendarmerie nationale
Durée de conservation des données	La durée de conservation varie selon la gravité des faits et l'âge de la personne impliquée (majeure ou mineure). Elle est au maximum de 25 ans. La durée de conservation maximale des traces et empreintes ainsi que des informations liées varie en fonction de la gravité de l'infraction, de la qualité de la personne concernée et du caractère national ou international de la procédure. ⇨ *Pour toutes les durées de conservation, voir l'article 5 du décret n°2015-1580 du 2 décembre 2015 :* *https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=87A5993225D9B991D8EB608513ACBCA4.tplgfr27s_2?idArticle=LEGIARTI000031564908&cidTexte=LEGITEXT000006065909&dateTexte=20190219*

Interconnexion avec d'autres fichiers ?	Les données enregistrées dans ce fichier peuvent être consultées, en vue notamment de faire l'objet de rapprochements, par les agents d'organismes de coopération internationale en matière de police judiciaire ou par les agents des services de police ou de justice d'Etats étrangers. *Article 4 du décret n°2011-157 modifiant le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.* *https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=E96CC9D5239F478C0F384EFB0F3032E7.tplgfr32s_1?idArticle=JORFARTI000023560651&cidTexte=JORFTEXT000023560638&dateTexte=29990101&categorieLien=id*
Quelle échelle ?	Nationale et internationale avec la communication des données
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - CESEDA, articles L 611-1-1, L 611-3 et L 611-4. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=2159FB6871BB7E9BB9790920469A9AD6.tplgfr38s_3?idSectionTA=LEGISCTA000006134417&cidTexte=LEGITEXT000006070158&dateTexte=20190211* - Décret n° 2015-1580 du 2 décembre 2015 modifiant le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4886DDC1651BC07B7B2EE2A7BFD2B79D.tplgfr32s_1?cidTexte=JORFTEXT000031560966&dateTexte=20151204* - Décret n°2011-157 du 7 février 2011 modifiant le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur. *https://www.legifrance.gouv.fr/eli/decret/2011/2/7/IOCC1014671D/jo/texte* - Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales, modifié. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006065909*
Comment obtenir communication et rectification des données ?	Pour accéder aux données au FAED il faut écrire au : *Service Central de la Police Technique et Scientifique* *31 avenue Franklin Roosevelt* *69134 Ecully cedex* Pour obtenir l'effacement des données du FAED : il faut faire une demande d'effacement au procureur de la République par LRAR ou déclaration au greffe. • en cas de refus d'effacement ou absence de réponse dans un délai de 3 mois : recours devant le JLD. • en cas de nouveau refus du JLD ou absence de réponse dans un délai de 2 mois : recours devant le Président de la chambre de l'instruction Le droit d'opposition prévu par *l'article 38 de la loi n° 78-17 du 6 janvier 1978* ne s'applique pas à ce traitement.
Sources	- CNIL, « Fichier automatisé des empreintes digitales « Faed » ». *https://www.cnil.fr/fr/faed-fichier-automatise-des-empreintes-digitales* - Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ».

Nom du fichier	**Fichier S**
Sens de l'acronyme	Atteinte à la sûreté de l'Etat, le fichier S constitue l'un des 21 sous-fichiers du FPR (fichier des personnes recherchées)
Objectif	Faciliter les recherches, les surveillances et les contrôles effectués, dans un cadre de police administrative ou judiciaire, par les services de police, de gendarmerie, des douanes ou de Tracfin (le « Traitement du renseignement et action contre les circuits financiers clandestins » est un service de renseignement placé sous l'autorité du Ministère de l'Action et des Comptes publics, qui concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme). La fiche S constitue un outil de renseignement permettant de collecter, pour le compte d'un service de renseignement prescripteur, des informations sur une personne identifiée. (*Sénat, Rapport d'information par le groupe de travail sur l'amélioration de l'efficacité des fiches S, 19 décembre 2018, voir lien dans les sources*)
Contenu des données	Structure du fichier : 11 catégories de fiches S (de S2 à S16, certaines catégories n'étant plus utilisées). Ces catégories ne correspondent pas à des niveaux de dangerosité mais renvoient à des profils et conduites à tenir (ex : les informations à recueillir ou les actions à entreprendre). ↳ Par exemple, lors d'un contrôle par la PAF dans un aéroport international, l'identité de la personne va être recherchée au sein du FPR. En cas de « hit » (réponse positive à une requête informatique) et d'existence d'une fiche au sein du FPR, le policier sera informé de l'existence d'une ou plusieurs consignes dans la conduite à tenir (ex : retenir l'intéressé et aviser le service demandeur). Contenu des données enregistrées : • état civil (nom, prénom, date et lieu de naissance, filiation), alias, sexe, nationalité, • signalement • photographie • motifs de la recherche • conduite à tenir en cas de découverte de la personne recherchée *Article 3 du décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées*
Critères d'inscription dans ce fichier	Les personnes faisant l'objet de recherches pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'Etat, dès lors que des informations ou des indices réels ont été recueillis à leur égard (*Décret n°2010-569 du 28 mai 2010, article 2, III, 8°*). *Précisions* : • la fiche S peut concerner toute personne de toute nationalité, présente sur le territoire national ou non • une personne « fichée S » n'a pas forcément commis une infraction
Date de création	15 mai 1996 (remplacé par le décret n°2010-569 du 28 mai 2010)
Autorité(s) compétente(s)	Direction générale de la police nationale et direction générale de la gendarmerie nationale du ministère de l'intérieur
Qui a accès à ce fichier ?	• Direction générale de la sécurité intérieure (DGSI) • Service central du renseignement territorial (SCRT) • Direction du renseignement de la préfecture de police de Paris (DRPP) • Direction générale de la gendarmerie nationale (DGGN)

Durée de conservation des données	2 ans, mais possible renouvellement de la fiche
Interconnexion avec d'autres fichiers ?	• Les signalements contenus dans le fichier S alimentent le SIS II (*Article 26 du Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération -SIS II-*) • API-PNR
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee. - Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022276189&dateTexte=20190219* - 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). *https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32006R1987*
Comment obtenir communication et rectification des données ?	Droit d'accès indirect (contrairement aux personnes inscrites dans les autres sous-fichiers du FPR) et droit de rectification ou d'effacement auprès de la CNIL. Le droit à l'information de la personne concernée par une collecte de données prévu par *l'article 32 de la loi n°78-17 du 6 janvier 1978 modifié par la loi n°2018-493 du 20 juin 2018* ne s'applique pas.
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - Sénat, Rapport d'information par le groupe de travail sur l'amélioration de l'efficacité des fiches S, 19 décembre 2018. *http://www.senat.fr/basile/visio.do?id=r8105530_6&idtable=r8105530_6|r8104929_12|r8104997_6|r8104757_4|r8105780|r8104914_13|r8105171_17|r8105531_7&_c=rapport+d%27information+fiche+s&rch=gs&de=20180306&au=20190306&dp=1+an&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn&isFirst=true#fn24*

Nom du fichier	**FNAEG**
Sens de l'acronyme	Fichier National Automatisé des Empreintes Génétiques
Objectif explicite	Le FNAEG (selon le site service public.fr) sert notamment à faciliter l'identification et la recherche des auteurs d'infractions (à l'aide de leur profil génétique) et des personnes disparues (à l'aide du profil génétique de leurs descendants/ascendants). ⇨ *Les empreintes génétiques sont les séquences d'ADN d'un individu, recueillies à partir de prélèvements effectués des échantillons organiques (sang, sperme, fragments de peau, de cheveux...).*
Objectif implicite/ Remarques	Selon Pierre Piazza, maître de conférence en sciences politiques à l'Université de Cergy Pontoise : « *Une loi du 17 juin 1998 fixait initialement comme objectif au Fnaeg l'identification des seuls auteurs d'infractions sexuelles. La loi du 15 novembre 2001 relative à la sécurité quotidienne en a étendu les enregistrements aux atteintes aux personnes et aux biens les plus graves. Puis, la loi du 18 mars 2003 pour la sécurité intérieure a prévu que pratiquement toutes les infractions pourraient donner lieu à un génotypage et qu'il serait possible de procéder à un prélèvement génétique sur les individus soupçonnés d'avoir commis un délit ou un crime.* » De plus, en 2005, avec le traité de Prüm relatif à la coopération policière et judiciaire en matière pénale entre les différents Etats membres de l'UE, des nouveaux destinataires ont été ajoutés à ce fichier et les conditions d'intégration au fichier ont été élargies. Les différents Etats membres peuvent ainsi consulter sous certaines conditions les données présentes dans le FNAEG.
Contenu des données	En plus des empreintes génétiques, d'autres données sont collectées : • nom, prénoms • date et lieu de naissance • sexe • le service ayant procédé à la signalisation • la date et le lieu d'établissement de la fiche signalétique • la nature de l'affaire et la référence de la procédure
Critères d'inscription dans ce fichier	L'enregistrement des empreintes se fait dans le cadre d'une enquête pour crime ou délit, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire. Les empreintes peuvent être celles de personnes : • non identifiées (empreintes issues de prélèvements sur les lieux d'une infraction) • identifiées (condamnées ou mises en cause par ex d'infractions sexuelles, crime contre l'humanité, trafic de stupéfiants, atteintes au libertés de la personne, etc.)
Date de création	18 mai 2000
Autorité(s) compétente(s)	La direction centrale de la police judiciaire rattachée au ministère de l'intérieur, sous le contrôle d'un magistrat
Qui a accès à ce fichier ?	• Les personnels habilités de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire, de la police nationale et ceux de la Gendarmerie nationale • Les personnes affectées au service central de préservation des prélèvements biologiques • Les agents spécialement habilités d'organismes de coopération internationale en matière de police judiciaire ou des services de police ou de justice d'Etats étrangers
Durée de conservation des données	• 40 ans : pour les données des personnes définitivement condamnées, décédées, disparues, ayant bénéficié d'une décision de classement sans suite, non-lieu, relaxe ou acquittement pour trouble mental • 25 ans : pour les données des personnes mises en cause pour notamment des infractions de nature sexuelle, les crimes contre l'humanité et les actes de terrorisme • 25 ans : pour les empreintes génétiques des ascendants ou descendants d'une personne disparue prélevées avec leur accord (disparition inquiétante ou suspecte)

Interconnexion avec d'autres fichiers ?	Avec la *décision 2008/615/JAI du Conseil relative à la coopération transfrontalière*, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, et prise dans le cadre du traité de Prüm, des dispositions relatives à la transmission d'informations sont prises entre les pays de l'UE. Ainsi : • Les pays de l'UE sont tenus de créer des fichiers nationaux d'analyses ADN aux fins des enquêtes relatives aux infractions pénales • Les données indexées, qui contiennent la partie non codante de l'ADN et un numéro de référence qui ne permet pas l'identification directe de la personne concernée doivent être mises à la disposition des autres pays de l'UE afin de permettre des consultations automatisées • Les points de contact nationaux offrent la possibilité d'effectuer des consultations par comparaison de profils ADN, uniquement au cas par cas et sur la base d'un système de concordance/non-concordance • Les pays de l'UE sont également tenus de garantir la disponibilité des données indexées provenant des systèmes automatisés nationaux d'identification par empreintes digitales • Les consultations s'effectuent par comparaison des données dactyloscopiques et, à l'instar des consultations de profils ADN, uniquement au cas par cas et selon un système de concordance/non-concordance
Quelle échelle ?	Nationale et communication des données au niveau européen
Lois qui régissent ce fichier	- 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. *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008D0615&from=FR* - Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Code de procédure pénale, articles 706-54 à 706-56-1. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=45ADC2A9A1B926EB23FA9A2024953044.tplgfr38s_3?idSectionTA=LEGISCTA000006138132&cidTexte=LEGITEXT000006071154&dateTexte=20190318* - Code de procédure pénale, articles R.53-9 à R.53-21. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=45ADC2A9A1B926EB23FA9A2024953044.tplgfr38s_3?idSectionTA=LEGISCTA000006137412&cidTexte=LEGITEXT000006071154&dateTexte=20190318* - Décret n°2000-413 du 18 mai 2000 modifiant le code de procédure pénale (deuxième partie : Décrets en Conseil d'État) et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9C8495769C8CFD4947BAEE0D824C0483.tplgfr35s_2?cidTexte=JORFTEXT000000399349&dateTexte=20000519* - Délibération de la CNIL n° 2008-113 du 14 mai 2008 portant avis sur un projet de décret en Conseil d'Etat modifiant le code de procédure pénale et relatif au fichier national des empreintes génétiques. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020788622* - Délibération de la CNIL n°02-008 du 7 mars 2002 relative à l'extension des conditions pour être inscrit dans ce fichier. *https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653512&fastReqId=1042459289&fastPos=8*
Comment obtenir communication et rectification des données ?	• Accès aux données du FNAEG : *Service Central de la Police Technique et Scientifique* *31 avenue Franklin Roosevelt* *69134 Ecully cedex* • Demande d'effacement des données : au procureur de la République par LRAR ou déclaration au greffe. ⇨ en cas de refus d'effacement : recours devant le JLD. ⇨ en cas de nouveau refus du JLD : recours devant le Président de la chambre de l'instruction. ↳ *Formulaire cerfa de demande d'effacement des données du FNAEG en ligne sur le site du ministère de la justice : https://www.service-public.fr/particuliers/vosdroits/R33424*
Sources	- P. Piazza, « L'extension des fichiers de sécurité publique », Revue Hermes, n°53, 2009. *https://www.cairn.info/revue-hermes-la-revue-2009-1-page-67.htm* - CNIL, « FNAEG : Fichier national des empreintes génétiques ». *https://www.cnil.fr/fr/fnaeg-fichier-national-des-empreintes-genetiques* - Service Public. *https://www.service-public.fr/particuliers/vosdroits/R33424*

Nom du fichier	**FPR**
Sens de l'acronyme	Fichier des Personnes Recherchées
Objectif explicite	Ce fichier recense toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique, afin de **faciliter les recherches effectuées par les services de police et de gendarmerie** à la demande des autorités judiciaires, militaires ou administratives. *Site de la CNIL : https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees*
Objectif implicite/ Remarques	Fichage de police, ayant une visée sécuritaire. Le fichier FPR est lié au système d'information Schengen, au niveau européen. Ce lien avec le SIS témoigne d'une « *extension des fichiers de sécurité publique* » selon Pierre Piazza, maître de conférence en sciences politiques à l'Université de Cergy Pontoise.
Contenu des données	Structure du FPR : division du FPR en 21 sous-fichiers en fonction du fondement juridique de la recherche, notamment : • E : police générale des étrangers • IT : interdiction de territoire • R : opposition à résidence en France • TE : opposition à l'entrée en France • S : sûreté de l'Etat • PJ : recherche de police judiciaire Données contenues dans le FPR : • Identité de la personne recherchée (état civil, sexe, nationalité...) • son signalement et éventuellement sa photographie • le motif de sa recherche • la conduite à tenir en cas de découverte des personnes recherchées (Site de la CNIL sur le FPR : *https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees* et *article 3 du Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées*)
Critères d'inscription dans ce fichier	• Judiciaires (exécution de mandats, de condamnation, d'un contrôle judiciaire, enquête de police judiciaire, etc.) • Administratifs (application de réglementations spécifiques de police administrative relatives aux étrangers -mesure d'expulsion, opposition à l'entrée sur le territoire-, à la législation fiscale ou la protection des personnes) • D'ordre public (prévention de menaces contre la sécurité publique ou la sûreté de l'État)
Date de création	15 mai 1996 (remplacé par le décret n°2010-569 du 28 mai 2010)
Autorité(s) compétente(s)	Direction générale de la police nationale et direction générale de la gendarmerie nationale du ministère de l'intérieur
Qui a accès à ce fichier?	• Les autorités judiciaires • Les services de police, de gendarmerie et des douanes • Les autorités administratives pour les seules recherches relevant de leurs attributions (préfectures et sous-préfectures) • Les services de police d'Etats liés à la France par une convention ou un accord international leur autorisant l'accès à tout ou partie des informations enregistrées dans le fichier des personnes recherchées (*Article 5 du décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées* et Rapport de recherche n°2 « Les fichiers de police et de renseignement en France », Jean-Marie COTTERET, Centre Français de Recherche sur le Renseignement, Octobre 2017, *https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf*)

Durée de conservation des données	• Les durées de conservation dépendent du motif d'enregistrement • Les radiations sont opérées sans délai en cas de découverte de la personne ou d'extinction du motif de l'inscription
Interconnexion avec d'autres fichiers ?	• Le FPR est toujours consulté avant la délivrance de permis de séjour • Inscription des étrangers fichés dans le FPR dans le SIS II (*Article 26 du Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération -SIS II-*) • API-PNR
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- Décret n° 2017-1219 du 2 août 2017 modifiant le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=8BD63D539F0374E39468E983AF6B898A.tplgfr27s_2?cidTexte=JORFTEXT000035355234&dateTexte=20170803* - Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022276189&dateTexte=&categorieLien=id* - Délibération de la CNIL n° 2009-587 du 12 novembre 2009 portant avis sur un projet de décret en Conseil d'Etat relatif au fichier des personnes recherchées (FPR). *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022276492* - Délibération de la CNIL n°2006-292 du 21 décembre 2006 portant avis sur le projet d'arrêté portant modification de l'arrêté du 15 mai 1996 modifié relatif au fichier des personnes recherchées. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023751042* - Délibération de la CNIL n° 95-051 du 25 avril 1995 portant avis conforme sur le projet de décret portant application au fichier des personnes recherchées des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653569* - Délibération de la CNIL n° 92-056 du 9 juin 1992 portant avis sur le projet d'arrêté relatif au fichier des personnes recherchées géré par le Ministère de l'Intérieur et le Ministère de la Défense. *https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017652618&fastReqId=1593598705&fastPos=1* - Délibération de la CNIL n° 88-120 du 8 novembre 1988 portant avis sur la mise en œuvre conjointe par le Ministère de l'Intérieur et le Ministère de la Défense du traitement automatisé d'informations nominatives relatif au fichier des personnes recherchées. *https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017652579&fastReqId=440998907&fastPos=1*
Comment obtenir communication et rectification des données ?	Le droit d'accès est direct pour : • les personnes inscrites pour des raisons n'intéressant par la sûreté de l'Etat (fiche "S"), la défense ou la sécurité publique (personnes faisant l'objet d'une décision judiciaire mentionnée à l'article 230-19 2 à 13 du code de procédure pénale) • les personnes mineures faisant l'objet d'une opposition à la sortie de territoire ou ayant quitté le domicile/soustraite à l'autorité des personnes en ayant la garde • les personnes débitrices de l'Etat • les personnes disparues • les personnes interdites de stade • les personnes mentionnées à l'article 2 IV du décret du 28 mai 2010 Les personnes doivent envoyer un courrier accompagné d'une copie d'un titre d'identité à : *Directeur central de la police judiciaire, Ministère de l'intérieur, Place Beauvau, 75800 Paris Cedex 08* Le droit d'accès est indirect dans les autres cas : il faut s'adresser à la CNIL.
Sources	- CNIL, « FPR : Fichier des personnes recherchées ». https://www.cnil.fr/fr/fpr-fichier-des-personnes-recherchees - Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - P. Piazza, « L'extension des fichiers de sécurité publique », Revue Hermes, n°53, 2009. *https://www.cairn.info/revue-hermes-la-revue-2009-1-page-67.htm* - Rapport de recherche n°2 « Les fichiers de police et de renseignement en France », Jean-Marie COTTERET, Centre Français de Recherche sur le Renseignement, Octobre 2017. *https://www.cf2r.org/wp-content/uploads/2017/10/RR-21-Fichiers-Police.pdf*

Nom du fichier	**GESTEL**
Sens de l'acronyme	Gestion de l'Eloignement
Objectif explicite	• Assurer la gestion de la mise en œuvre opérationnelle, matérielle et logistique des mesures d'éloignement, au sein de la direction centrale de la police aux frontières *ex : organisation du transport, réservations hôtelières, mise en place d'une escorte…* • Améliorer l'exécution des mesures d'éloignement par la dématérialisation des échanges d'informations externes et internes • Garantir le suivi de procédures d'éloignement et en faciliter le contrôle *Article R. 611-7 du CESEDA*
Objectif implicite / Remarques	Lutte contre l'immigration irrégulière
Contenu des données	• Données relatives au service à l'origine de la demande d'éloignement : préfecture, numéro de dossier, date et heure de saisine... • Données relatives à l'état civil du ressortissant étranger faisant l'objet de la mesure d'éloignement : numéro AGDREF, nom, prénoms, nationalité... • Données relatives à la situation administrative du ressortissant étranger faisant l'objet de la mesure d'éloignement : décisions administratives (OQTF, ITF...), documents d'identité... • Données relatives à la requête de la demande d'éloignement : destination (pays et ville), vecteur souhaité pour le transport, date sollicitée... • Renseignements complémentaires : escorte, accompagnants, refus antérieurs d'embarquer. • Données relatives aux itinéraires empruntés et les réservations hôtelières : nom du transporteur, jour et heure de départ et d'arrivée... • Données relatives au documents numérisés relatifs à la personne concernée par la mesure d'éloignement : fiche pénale, accord de réadmission, main courante... ↳ *Liste exhaustive des données à l'annexe 6-5 du CESEDA* : *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=924416F90854098022C8C529127970F4.tplgfr41s_2?idSectionTA=LEGISCTA000038108273&cidTexte=LEGITEXT000006070158&dateTexte=20190225*
Critères d'inscription dans ce fichier	Faire l'objet d'une mesure d'éloignement
Date de création	07 février 2019
Autorité(s) compétente(s)	Ministre de l'intérieur (Direction générale de la police nationale)

Qui a accès à ce fichier ?	Autorités pouvant accéder aux données : • les agents de la direction centrale de la police aux frontières • les agents des préfectures Autorités pouvant être destinataires des données : • le contrôleur général des lieux de privation de liberté • les agents et militaires de la direction générale de la gendarmerie nationale • les agents de la direction générale de la police nationale • les agents de la direction générale des douanes et droits indirects • les agents de la direction générale des étrangers en France • le prestataire voyagiste agréé par le ministère de l'Intérieur • les autorités du pays de transit ou de destination chargées d'autoriser et de faciliter l'éloignement • les compagnies aériennes ou maritimes assurant la prise en charge de l'éloignement *Article R. 611-19 du CESEDA*
Durée de conservation des données	• Pendant une durée de deux ans à compter de la date de leur enregistrement pour permettre l'exécution de la mesure d'éloignement. • Pendant une durée de six mois après la date d'exécution effective de la mesure d'éloignement. A l'issue de ces délais, ces données à caractère personnel et informations sont conservées pendant une durée de six ans et uniquement accessibles aux agents relevant de la cellule opérationnelle de l'éloignement de la direction centrale de la police aux frontières. Les données à caractère personnel et informations relatives aux personnes dont la mesure d'éloignement a été annulée, abrogée ou retirée sont effacées du traitement par la direction centrale de la police aux frontières dès qu'elle en a connaissance. *Article R. 611-20 du CESEDA*
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- CESEDA, articles R. 611-17 à R. 611-22. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=924416F90854098022C8C529127970F4.tplgfr41s_2?idSectionTA=LEGISCTA000038108321&cidTexte=LEGITEXT000006070158&dateTexte=20190225* - Décret n° 2019-81 du 6 février 2019 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « Gestion de l'éloignement » (GESTEL) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile. *http://www.gisti.org/IMG/pdf/decret_2019-2-6_norintd1829052d.pdf* - Délibération de la CNIL n° 2018-162 du 17 mai 2018 portant avis sur un projet de décret autorisant un traitement automatisé de données à caractère personnel dénommé « Gestion de l'éloignement ». *https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038104253*
Comment obtenir communication et rectification des données ?	Ces droits s'exercent auprès de la direction générale de la police nationale. *Article R. 611-22 du CESEDA*
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - Site du GISTI, voir ci-dessus les « Lois qui régissent ce fichier ».

Nom du fichier	**GIPI**
Sens de l'acronyme	Gestion Informatisée des Procédures d'Immigration
Objectif explicite	• Faciliter la gestion des procédures de non-admission des étrangers qui ne remplissent pas les conditions d'entrée dans l'espace de libre circulation des personnes entre les Etats signataires de l'accord de Schengen. • Permet le traitement et la gestion du suivi des amendes infligées aux entreprises de transport. *Article 1 de l'arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration »* *Précision* : le GIPI est le logiciel utilisé par la PAF pour délivrer le document de refus d'entrée et la notification de maintien en zone d'attente.
Objectif implicite/ Remarques	Succède au FNAD (Fichiers des non-admis).
Contenu des données	• Données relatives au passager : civilité, nom, prénom, genre, date et lieu de naissance, situation de famille, nationalité, pays de naissance, lieu de résidence, profession, langue parlée, numéro d'enregistrement pour le dossier de maintien en zone d'attente, date et résultat de l'examen osseux. • Données relatives à l'accompagnant : date de naissance, genre, nom, prénom, nationalité, lieu de naissance, date et résultat de l'examen osseux. • Données relatives à la procédure mise en œuvre : . procédure de maintien en zone d'attente . procédure de demande d'asile . procédure de présentation de l'étranger non admis devant les juridictions compétentes . procédure de réadmission dans l'espace Schengen • Données relatives à l'hébergement de la personne non-admise : compagnie aérienne concernée, aérogare... • Données relatives aux documents de voyage : type, identifiant et pays de délivrance du document, caractère authentique ou non, numéro du visa Schengen... • Données relatives à l'interprète : nom, prénom, langue parlée... • Données relatives aux pénalités financières infligées à l'entreprise de transport : libellé de la compagnie... ↳ *Lien vers le contenu exhaustif des données présentes dans ce fichier :* *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027169411*
Critères d'inscription dans ce fichier	S'être vu refuser l'entrée sur le territoire Schengen aux frontières aériennes, terrestres ou maritimes en France
Date de création	14 février 2013
Autorité(s) compétente(s)	Le directeur général de la police nationale

Qui a accès à ce fichier ?	• Les agents de la police nationale affectés à la direction centrale de la police aux frontières • Les agents des services de la direction générale des étrangers en France du ministère de l'intérieur • Les agents de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur *Article 4 de l'arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration »*
Durée de conservation des données	Trois mois à compter de la clôture du dossier *Article 3 de l'arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration »*
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration ». *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027169411* - Délibération n° 2012-431 de la Commission nationale de l'informatique et des libertés en date du 6 décembre 2012 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration ». *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027169750&categorieLien=id*
Comment obtenir communication et rectification des données ?	Les droits d'accès et de rectification s'exercent auprès de la direction centrale de la police aux frontières et ils sont régis par la règlementation sur la protection des données personnelles. *Article 6 de l'arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration »*
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - Rapport du Contrôleur général des lieux de privation de liberté de la visite de la zone d'attente de l'aéroport Roissy Charles-de-Gaulle, 2013. *http://www.cglpl.fr/2015/rapport-de-la-deuxieme-visite-de-la-zone-dattente-de-laeroport-de-roissy-charles-de-gaulle-val-doise/*

Nom du fichier	**INEREC**
Sens de l'acronyme	Instruction et recours (Application informatique relative à la gestion des demandeurs d'asile et de l'état civil des personnes protégées. Elle constitue la base de données d'enregistrement des demandes d'asile en France).
Objectif	Permettre la **gestion des demandes d'asile par l'OFPRA**, en permettant l'échange d'informations avec les préfectures et le ministère de l'intérieur sur la situation des demandeurs d'asile (D. Lochak, « Des fichiers pour gérer, contrôler et surveiller les étrangers », Plein droit, n°71, 2006. *https://www.cairn.info/revue-plein-droit-2006-4-page-24.htm)*
Contenu des données	• Identité du demandeur d'asile : nom, prénoms, sexe, date et lieu de naissance, situation de famille, nationalité, adresse • Situation administrative : nature des documents d'identité versés au dossier, date de dépôt de la demande • Classification du dossier: identifiant, vitesse d'examen • Décision sur la demande : nature, date *Article 2 de l'arrêté du 5 novembre 1990 relatif à une opération d'automatisation des formalités administratives qui découlent du dépôt d'une demande de statut auprès de l'OFPRA et à la création d'un service télématique, de messageries électroniques et d'édition de statistiques.*
Critères d'inscription dans ce fichier	Etre demandeur d'asile
Date de création	5 novembre 1990
Autorité(s) compétente(s)	L'OFPRA et la CNDA (Cour Nationale du Droit d'Asile)
Qui a accès à ce fichier ?	• L'OFPRA • La CNDA • La préfecture du lieu de résidence du demandeur d'asile • Le ministre de l'intérieur • Le service social d'aide aux émigrants • Les Assedic • La délégation pour la France du haut-commissariat pour les réfugiés (pour ce qui est des décisions de rejet ou de retrait) *Article 4 de l'arrêté du 5 novembre 1990*
Durée de conservation des données	Pas d'information pour la conservation des données d'INEREC mais pour celles concernant les fichiers DNA et ADGREF 2 avec lesquelles le fichier INEREC est partiellement interconnecté (Voir DNA et ADGREF 2)
Interconnexion avec d'autres fichiers ?	• Selon l'arrêté du 5 novembre 1990, le fichier ne peut faire l'objet d'aucune cession, interconnexion, mise en relation ou rapprochement avec un autre fichier • Or, dans les faits, il y a une interconnexion partielle avec les fichiers AGDREF 2 et DNA *https://www.lacimade.org/faq/abecedaire-des-migrations/*
Quelle échelle ?	Nationale

Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2018-493 du 20 juin 2018. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Arrêté du 5 novembre 1990 relatif à une opération d'automatisation des formalités administratives qui découlent du dépôt d'une demande de statut auprès de l'OFPRA et à la création d'un service télématique, de messageries électroniques et d'édition de statistiques. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000344394&fastPos=5&fastReqId=1730468711&categorieLien=cid&oldAction=rechTexte* - Délibération de la CNIL du 10 juillet 1990 n° 90-88 relative à un traitement automatisé d'informations nominatives concernant la gestion des formalités administratives relevant de l'OFPRA. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652997*
Comment obtenir communication et rectification des données ?	Le droit d'accès s'exerce auprès de l'OFPRA. *Article 3 de l'arrêté du 5 novembre 1990*
Sources	- D. Lochak, « Des fichiers pour gérer, contrôler et surveiller les étrangers », Plein droit, n°71, 2006. *https://www.cairn.info/revue-plein-droit-2006-4-page-24.htm* - Site internet de La CIMADE, Rubrique « Abécédaire des migrations ». *https://www.lacimade.org/faq/abecedaire-des-migrations/*

Nom du fichier	**OSCAR**
Sens de l'acronyme	Outil de Statistique et de Contrôle de l'Aide au Retour
Objectif explicite	• Déceler une demande présentée par une personne ayant déjà bénéficié de l'aide au retour, le cas échéant sous une autre identité • Effectuer le suivi administratif, budgétaire et comptable des procédures d'aide au retour gérées par l'Office français de l'immigration et de l'intégration • Etablir des statistiques relatives à ces procédures et à leur exécution *Article R. 611-35 du CESEDA*
Objectif implicite/ Remarques	Objectif implicite d'entraver la liberté de circulation de Roms roumains ou bulgares ayant déjà fait l'objet d'une aide au retour. Bien que le fichier OSCAR vise l'ensemble des étranges susceptibles de bénéficier d'une aide au retour, plusieurs associations ont relevé qu'en pratique ce sont majoritairement les Roms, venant de Bulgarie ou de Roumanie, qui sont visés, représentant 90% des personnes se voyant attribuer une aide au retour. Ce chiffre s'explique par la stratégie des pouvoirs publics consistant lors de l'évacuation d'un campement de Roms de leur forcer la main pour qu'ils acceptent l'aide au retour, sous peine d'encourir des poursuites pénales. (Communiqué commun Gisti / Iris / Ligue des Droits de l'Homme, « Oscar ou le déni de citoyenneté européenne des Roms », 21 septembre 2010. *https://www.ldh-france.org/wp-content/uploads/IMG/pdf/Communique_commun_Oscar_note_complementaire.pdf)*
Contenu des données	• Les images numérisées des empreintes des dix doigts du bénéficiaire et de ses enfants mineurs d'au moins 12 ans • Les données à caractère personnel relatives aux bénéficiaires, notamment son identité ou sur la gestion administrative et comptable du dossier de demande d'aide au retour, ou encore l'organisation du voyage ↳ *Liste exhaustive des données à l'annexe 6-8 du CESEDA* : *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=5F037C4188935C6078884F5495D9FAEA.tplgfr22s_2?idSectionTA=LEGISCTA000021210468&cidTexte=LEGITEXT000006070158&dateTexte=20190225* Le traitement OSCAR ne comporte pas de dispositif d'identification nominative à partir des empreintes, c'est-à-dire qu'elles ne permettent pas d'identifier directement les étrangers concernés, sauf en cas de réquisition judiciaire. Il ne comporte pas non plus de dispositif de reconnaissance faciale à partir de la photographie.
Critères d'inscription dans ce fichier	Les données, et notamment les empreintes digitales, sont enregistrées dans le traitement OSCAR dès le dépôt du dossier de demande d'aide au retour par la personne concernée, par les agents de l'OFII. Cependant, ces données biométriques ne sont enregistrées qu'aux fins de comparaison avec les empreintes déjà enregistrées dans le système, afin de déterminer si le demandeur a déjà bénéficié d'une telle aide, sous une même identité ou sous une autre. Ainsi, les empreintes relatives aux demandeurs d'une aide dont la demande a été refusée, ou qui ont renoncé au bénéfice de l'aide avant le premier versement, sont effacées sans délai. **Seules les empreintes digitales des bénéficiaires de l'aide sont donc conservées dans le traitement OSCAR**, conformément à ce qui est prévu par la loi. Il en est de même pour les autres informations enregistrées dans le traitement, qui sont effacées sans délai lorsque l'OFII refuse une aide sollicitée ou lorsque l'intéressé renonce au bénéfice de celle-ci.
Date de création	26 octobre 2009
Autorité(s) compétente(s)	L'OFII

Qui a accès à ce fichier ?	⇨ Les agents de l'OFII chargés de la mise en œuvre du dispositif d'aide au retour sont les seuls à avoir un accès direct. ⇨ Possible communication de données par l'intermédiaire des agents de l'OFII aux personnes suivantes : • Les agents préfectoraux compétents pour l'application de la réglementation relative aux étrangers, afin d'assurer le suivi administratif des procédures d'attribution des aides au retour • Les agents des ambassades et des consulats français à l'étranger afin de pouvoir assurer le suivi de la procédure après le départ en France • Les personnels des organismes partenaires de l'OFII à la seule fin de la réalisation des missions qui leur sont confiées par les conventions les liant à cette dernière
Durée de conservation des données	• Lorsque l'aide au retour volontaire est accordée, l'ensemble des données enregistrées dans le fichier OSCAR sont conservées pendant cinq ans à compter de la date de la décision de l'OFII • Lorsque l'aide au retour volontaire est refusée ou l'intéressé y renonce, les données sont effacées sans délai
Interconnexion avec d'autres fichiers ?	Non
Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- CESEDA, articles L. 611-3 et R. 611-35 à 41. *https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006335274&cidTexte=LEGITEXT000006070158&dateTexte=20091125* et *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=DA8989699A3F78E2B6A0FAEEFB8615F0.tplgfr22s_2?idSectionTA=LEGISCTA000021210439&cidTexte=LEGITEXT000006070158&dateTexte=20190318* - Décret n° 2009-1310 du 26 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour géré par l'Office français de l'immigration et de l'intégration. *https://www.legifrance.gouv.fr/eli/decret/2009/10/26/IMIK0922946D/jo/texte* - Délibération de la CNIL n° 2009-468 du 16 juillet 2009 portant avis sur le projet de décret portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour financé par l'Office français de l'immigration et de l'intégration et modifiant la partie réglementaire du code de l'entrée et du séjour des étrangers et du droit d'asile. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021205064*
Comment obtenir communication et rectification des données ?	Les droits d'accès et de rectification aux données qui les concernent, s'exercent directement auprès du directeur général de l'OFII. Le délai moyen prévu pour la communication des informations demandées est de un mois.
Sources	- Site de la LDH, « Oscar ou le déni de citoyenneté européenne des Roms ». *https://www.ldh-france.org/Oscar-ou-le-deni-de-citoyennete/* - CNIL, « OSCAR : Outil de Statistique et de Contrôle de l'Aide au Retour ». *https://www.cnil.fr/fr/oscar-outil-de-statistique-et-de-controle-de-laide-au-retour*

Nom du fichier	**RMV 2**
Sens de l'acronyme	Réseau Mondial Visa 2 *Le fichier RMV2 a remplacé le fichier RMV*
Objectif explicite	**L'instruction des demandes de visas par les consulats**, en permettant l'échange d'informations avec le ministère de l'intérieur et les autorités des États Schengen. Le fichier est consulté à chaque instruction de dossier de demande de visa, dans lequel sont enregistrées toutes les demandes de visas faites dans les consulats français de par le monde. Cette consultation permet de savoir si le demandeur est signalé dans une des autres bases de données auxquelles donne accès le réseau (G. Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs », cahiers internationaux de sociologie, n°125, 2008, *https://www.cairn.info/revue-cahiers-internationaux-de-sociologie-2008-2-page-263.htm)*
Objectif implicite/ Remarques	Opérer un contrôle accru des personnes étrangères en croisant les fichiers des différentes demandes d'entrées sur le territoire qui ont été faites mais aussi les données des fichiers européens de contrôle des visas et de l'immigration (VIS et SIS).
Contenu des données	Structure du fichier : plusieurs sous-fichiers : • Le fichier des demandes, délivrance et refus de visas • Le fichier central d'attention : enregistrement des informations relatives aux cas de fraude, aux personnes frappées par une mesure d'expulsion ou dont la venue en France constitue une menace pour l'ordre public, des signalements répertoriés dans le SIS • Le fichier consulaire d'attention : alimenté par les consulats qui enregistrent les signalements favorables ou défavorables • Le fichier des "répondants signalés" : personnes ou organismes accueillant les demandeurs de visa lors de leur séjour en France • Le fichier des titres de voyage répertoriés : données concernant les titres irrecevables car déclarés volés, perdus, annulés ou falsifiés • Le fichier des demandes de carte de commerçant • Le fichier des interventions : enregistrement des cas dans lesquels une demande de visa a été appuyée par un intervenant extérieur • Le fichier du suivi du contentieux Contenu des données : • données relatives au demandeur de visa : photographie de face, images et minuties des empreintes digitales des dix doigts à plat... • données relatives au suivi du visa : visa délivré, abandon de l'examen du visa, prolongation... ↳ *Liste exhaustive des données : Annexe 6-3 du CESEDA* *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=5F037C4188935C6078884F5495D9FAEA.tplgfr22s_2?idSectionTA=LEGISCTA000006115078&cidTexte=LEGITEXT000006070158&dateTexte=20190225*
Critères d'inscription dans ce fichier	Etre demandeur de visa
Date de création	22 août 2001
Autorité(s) compétente(s)	Le ministère des affaires étrangères, le ministère de l'intérieur et les autorités centrales des pays Schengen dans la limite de leurs attributions
Qui a accès à ce fichier ?	• Les agents des services centraux du ministère des affaires étrangères, du ministère chargé de l'immigration, du ministère de l'intérieur, du ministère chargé du budget, du ministère de la défense • Les agents des missions diplomatiques et postes consulaires • Les agents des préfectures et des représentations de l'Etat en Nouvelle-Calédonie, en Polynésie française et aux îles Wallis-et-Futuna • Les consulats français • Les ambassades françaises • Les autorités centrales des pays Schengen, dans la limite de leurs attributions • Les agents de l'OFII • Les agents de la commission de recours contre les décisions de refus de visa

	↳ *Liste exhaustive* : Article 5 de l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires, modifié par l'arrêté du 24 novembre 2009. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000021370340*
Durée de conservation des données	Les données à caractère personnel enregistrées au fichier des demandes, délivrances et refus de visas sont conservées pendant une période maximale de cinq ans à compter : • de la date d'expiration du visa, en cas de délivrance d'un visa • de la nouvelle date d'expiration du visa, en cas de prorogation d'un visa • de la date de la création du dossier de demande en cas de retrait, de clôture ou d'interruption de la demande • de la date de la décision en cas de refus, d'annulation, de réduction ou de retrait d'un visa Les données à caractère personnel enregistrées au fichier central d'attention, au fichier consulaire d'attention, au fichier des répondants signalés et au fichier des interventions sont conservées pendant une durée maximale de cinq ans. *Article 4-1 de l'arrêté du 24 novembre 2009 modifiant l'arrêté du 22 août 2001 portant création du RMV2*
Interconnexion avec d'autres fichiers ?	L'application informatique RMV 2 permet, lors du dépôt d'une demande de visa, l'interrogation systématique : • du fichier SIS • du VIS • du fichier d'authentification des actes d'état civil *Article 2 de l'arrêté du 24 novembre 2009 modifiant l'arrêté du 22 août 2001 portant création du RMV2*
Quelle échelle ?	Nationale et européenne par le croisement des fichiers
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Arrêté du 24 novembre 2009 modifiant l'arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=5F037C4188935C6078884F5495D9FAEA.tplgfr22s_2?cidTexte=JORFTEXT000021369746&dateTexte=20170129* - Arrêté du 22 août 2001 portant création d'un traitement informatisé d'informations nominatives relatif à la délivrance des visas dans les postes diplomatiques et consulaires. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000771780&categorieLien=id*
Comment obtenir communication et rectification des données ?	Le droit d'accès aux informations collectées lors du dépôt de la demande de visa s'exerce en application de *l'article 39 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2018-493 du 20 juin 2018*, auprès du consulat ou de l'ambassade où la demande de visa a été déposée. Le droit d'accès aux informations figurant dans les fichiers d'opposition ou d'attention s'exerce en application de *l'article 39 de la loi précitée*, auprès de la Commission nationale de l'informatique et des libertés.
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - La Cimade, Rapport d'observation, « Visa refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas », juillet 2010. *https://www.lacimade.org/wp-content/uploads/2015/12/Rapport_VisaRefuse_PremierePartie_definitif.pdf* - D. Lochak, « Des fichiers pour gérer, contrôler et surveiller les étrangers » , Plein droit, n°71, 2006. *https://www.gisti.org/spip.php?article4367* - G. Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs », cahiers internationaux de sociologie, n°125, 2008. *https://www.cairn.info/revue-cahiers-internationaux-de-sociologie-2008-2-page-263.htm*

Nom du fichier	**SILCF**
Sens de l'acronyme	Système Informatisé de Lutte Contre les Fraudes
Objectif	La **direction générale des douanes et droits indirects** met en œuvre un traitement automatisé comportant des informations nominatives dénommé Système d'information de lutte contre la fraude (SILCF), dont la finalité est **l'aide à la bonne exécution des missions de recherche, de constatation, de poursuite et de répression des fraudes** qui lui sont confiées, notamment dans le cadre de ses compétences en matière économique, fiscale et de protection de l'espace national et communautaire. Les fraudes mentionnées au premier alinéa sont : • les délits et contraventions prévus et réprimés par le code des douanes • les délits prévus et réprimés par le code général des impôts en matière de contributions indirectes ou de réglementations assimilées aux contributions indirectes • les délits et contraventions que la douane est habilitée à constater et, le cas échéant, à rechercher, en application des dispositions contenues notamment dans le code de la consommation, le code rural, le code de l'aviation civile, le code du travail, le code de la propriété intellectuelle, le code monétaire et financier, le code de la route, le code de l'environnement, le code des ports maritimes, le code des postes et télécommunications, le code de la santé publique et le code du travail maritime. *Article 1 de l'arrêté du 1 juillet 2003 portant création à la direction générale des douanes et droits indirects d'un système informatisé concourant au dispositif de lutte contre les fraudes :* *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=06A700DD83A6D280AB6016479D8E525C.tplgfr34s_2?cidTexte=JORFTEXT000000239747&dateTexte=20180907*
Contenu des données	Les catégories d'informations directement ou indirectement nominatives susceptibles d'être enregistrées sont : • au titre de l'identification des personnes physiques impliquées dans une fraude constatée ou soupçonnée ou ayant déposé une déclaration : noms, prénoms, pseudonymes, sexe, situation de famille, date et lieu de naissance, nationalité, nature, numéro et lieu de délivrance des pièces d'identité, adresse de la résidence principale et des autres résidences, profession, employeur • au titre de l'identification et de l'activité des personnes morales impliquées ou soupçonnées de fraude : raison sociale, n° SIRET, adresse, numéros de téléphone et de télécopieur, adresses postales et électroniques, identifiant activité, éléments de comptabilité, importations et exportations • au titre de la description des circonstances de la fraude constatée ou soupçonnée : marchandises de fraude, marchandises ayant servi à masquer la fraude, procédés de fraude, circonstances, moyens de communication, identification, description, propriété, usage et mouvements des vecteurs de transport • la nature et la qualification de l'infraction constatée ou soupçonnée • au titre des suites administratives et judiciaires réservées aux constatations de fraude : date de saisine de l'autorité judiciaire, suivi et déroulement des actions contentieuses, montant et qualification des sommes liquidées, étapes de la procédure de recouvrement • pour les déclarations de mouvements de sommes, titres ou valeurs : sens du transfert (entrée ou sortie), provenance et destination, sommes déclarées (nature, montant, monnaie), identification du propriétaire des fonds ou de son représentant ainsi que la désignation du lieu de franchissement de la frontière aérienne ou maritime ou de la région géographique de franchissement de la frontière terrestre, la date et le numéro d'enregistrement lorsque la déclaration est souscrite par internet
Critères d'inscription dans ce fichier	Les informations nominatives qui font l'objet d'un enregistrement concernent : • Les personnes à l'encontre desquelles existent une ou plusieurs raisons plausibles de leur implication dans une fraude, qui sont mentionnées dans une fiche de soupçon de fraude ou une demande d'enquête • Les personnes détentrices d'une marchandise qui fait l'objet d'une demande d'analyse • Les personnes ayant déposé auprès de la douane une déclaration en application du Règlement (CE) n° 1889/2005 du Parlement européen et du Conseil du 26 octobre 2005 relatif aux contrôles de l'argent liquide entrant ou sortant de la Communauté, d'une part, ou en application de l'article 464 du code des douanes, d'autre part • Les personnes ayant déposé auprès de la douane une déclaration de transfert de sommes, titres ou valeurs à destination ou en provenance de l'étranger à Saint-Pierre-et-Miquelon en application de l'article L. 721-2 du code monétaire et financier, à Mayotte en application de l'article L. 731-3 du même code, en Nouvelle-Calédonie en application de l'article L. 741-4 du même code, en Polynésie française en application de l'article L. 751-4 du même code et dans les îles Wallis et Futuna en application de l'article L. 761-3 du même code • Les personnes dont la participation à une fraude réalisée a fait l'objet d'un procès-verbal de constatation ou de saisie, d'un règlement transactionnel ou d'un autre acte de constatation ☞ *Liste des données exhaustives sur le site internet de Légifrance* : *https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=82502AA5455E3FF27EC26028332B5553.tplgfr34s_2?idArticle=LEGIARTI000026912898&cidTexte=LEGITEXT000005634896&dateTexte=20180907*

Date de création	01 juillet 2003
Autorité(s) compétente(s)	La direction générale des douanes et droits indirects
Qui a accès à ce fichier ?	Peuvent se connecter au SILCF suivant une procédure d'identification individuelle et accéder aux informations qu'ils ont à connaître dans le cadre de leurs attributions fonctionnelles et de leurs compétences territoriales respectives les agents suivants de la direction générale des douanes et droits indirects : • Les agents dûment habilités des services spécialisés dans l'analyse du risque et le traitement du renseignement sont seuls destinataires des informations relatives aux risques de fraude aussi longtemps que ces services ne les ont pas validées en vue de leur utilisation et de leur diffusion à des fins de contrôle ou d'enquête sous la forme d'avis de fraude ou de fiches d'enquête. Toutefois, les agents des services ayant signalé un risque de fraude conservent la possibilité d'accéder aux informations relatives à ce signalement • Les agents dûment habilités des services d'enquête sont destinataires des informations relatives aux enquêtes qui leur sont confiées. Les agents des autres services sont informés qu'une personne fait l'objet d'une demande d'enquête • Tous les agents, y compris les agents des douanes habilités à effectuer des enquêtes judiciaires, investis d'une mission de lutte contre la fraude et ayant reçu une habilitation peuvent être destinataires des informations relatives aux constatations réalisées, aux résultats des analyses effectuées par les laboratoires des douanes et des informations contenues dans les avis de fraude • Les agents habilités des laboratoires des douanes sont destinataires des demandes d'analyse et d'expertise de marchandises qui leur sont confiées • Les agents dûment habilités des services du contentieux et comptables sont seuls destinataires des informations contenues dans le volet des fiches de constatations réalisées relatif à la gestion du contentieux et au suivi des procédures de recouvrement • Les agents dûment habilités de l'administration centrale en charge du pilotage de la lutte contre la fraude accèdent à l'ensemble des informations conservées dans le SILCF • Les autorités hiérarchiques accèdent à l'ensemble des informations relatives à l'activité des services qui relèvent de leur compétence • En outre, les agents dûment habilités des services spécialisés dans l'analyse du risque et le traitement du renseignement ainsi que ceux investis d'une mission de lutte contre la fraude sont destinataires des données relatives aux déclarations déposées en application du règlement (CE) n° 1889/2005 du Parlement européen et du Conseil du 26 octobre 2005 relatif aux contrôles de l'argent liquide entrant ou sortant de la Communauté ainsi qu'en application de l'article 464 du code des douane, d'une part, et des articles L. 721-2, L. 731-3, L. 741-4, L. 751-4 et L. 761-3 du code monétaire et financier, d'autre part
Durée de conservation des données	• Trois ans pour les données nominatives relatives aux risques de fraude, aux demandes d'enquête, aux résultats des analyses de laboratoires (le délai de 3 ans peut être renouvelé une fois pour les demandes d'enquête si les premières diligences ont été accomplies ou que, pour les données relatives aux risques de fraude, des éléments objectifs nouveaux concernant la même personne sont intervenus) • Dix ans pour les informations nominatives relatives aux fraudes constatées, à compter de l'année de la constatation • Cinq ans pour les données et informations relatives au respect de l'obligation déclarative des mouvements de sommes, titres ou valeurs, à compter de leur introduction dans le traitement • Au-delà des délais précités, les données informatiques nominatives contenues dans les dossiers sont éliminées du système informatique et conservées sur un support non destructible pendant une durée de cinq ans pour la réalisation d'audits hiérarchiques ou à des fins historiques. Elles peuvent également être utilisées par la CNIL et les autorités judiciaires *Article 5 de l'arrêté du 7 novembre 2012*
Interconnexion avec d'autres fichiers ?	Avec le fichier API-PNR

Quelle échelle ?	Nationale
Lois qui régissent ce fichier	- Arrêté du 31 janvier 2017 modifiant l'arrêté du 1er juillet 2003 portant création d'un système informatisé de lutte contre les fraudes. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=06A700DD83A6D280AB6016479D8E525C.tplgfr34s_2?cidTexte=JORFTEXT000033977066&dateTexte=20170203* - Arrêté du 7 novembre 2012 autorisant la création d'un traitement automatisé dénommé « DALIA » et modifiant l'arrêté du 1er juillet 2003 portant création d'un système informatisé de lutte contre les fraudes. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=06A700DD83A6D280AB6016479D8E525C.tplgfr34s_2?cidTexte=JORFTEXT000026872274&dateTexte=20180907* - Arrêté du 1 juillet 2003 portant création à la direction générale des douanes et droits indirects d'un système informatisé concourant au dispositif de lutte contre les fraudes. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=06A700DD83A6D280AB6016479D8E525C.tplgfr34s_2?cidTexte=JORFTEXT000000239747&dateTexte=20180907* - Délibération de la CNIL n°03-029 du 22 mai 2003 concernant la création par la direction générale des douanes et droits indirects d'un système d'information de lutte contre la fraude. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653785*
Comment obtenir communication et rectification des données ?	Les droits d'accès et de rectification (*articles 38 et suivants de la loi n°78-17 du 6 janvier 1978 modifiés par les lois n°2004-801 du 6 août 2004 et n°2018-493 du 20 juin 2018*) s'exercent auprès des directions régionales des douanes. Lorsque la douane estime que certaines des informations demandées, ou leur totalité, intéressent la sûreté de l'Etat, la défense ou la sécurité publique au sens de *l'article 39 de la loi précitée modifié par la loi n°2018-493 du 20 juin 2018* ou sont couvertes par une règle de secret résultant d'une convention internationale, elle transmet la demande à la Commission nationale de l'informatique et des libertés. Celle-ci délimite, le cas échéant, les informations qui sont communicables de plein droit par application de l'article 34 précité et celles qui relèvent de la procédure de l'article 39 modifié. *Article 9 de de l'arrêté du 7 novembre 2012*
Sources	- Légifrance, voir ci-dessus « Lois qui régissent ce fichier ».

Nom du fichier	TAJ
Sens de l'acronyme	Traitement d'Antécédents Judiciaires *(Anciens fichiers STIC et JUDEX)*
Objectif explicite	Le TAJ est constitué des données recueillies notamment par la police, la gendarmerie nationale et les agents des douanes judiciaires. Il est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et dans le cadre d'enquêtes administratives (enquêtes préalables à certains emplois publics ou sensibles par exemple). Site du service public sur le TAJ : *https://www.service-public.fr/particuliers/vosdroits/F32727*
Objectif implicite/ Remarques	Ce fichier a une visée sécuritaire au détriment des libertés individuelles. Marc Duranton et Jean-Philippe Foegle, « Fichage partout, oubli nulle part ? Le Conseil d'Etat ouvre un boulevard au fichier « TAJ » », La Revue des droits de l'homme, Actualités Droits-Libertés, juillet 2014. *https://journals.openedition.org/revdh/849*
Contenu des données	<u>Personnes mises en causes en tant qu'auteures ou complices de crimes :</u> • identité • situation familiale • nationalité, adresse • adresse de messagerie électronique • numéros de téléphone • date et lieu de naissance • profession • état de la personne • signalement • photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale <u>Concernant les victimes :</u> • identité • date et lieu de naissance • situation familiale • nationalité • adresses • profession • état de la personne • pour les personnes morales : raison sociale, enseigne commerciale, sigle, forme juridique, lieu du siège social, secteur d'activité, adresses, numéros de téléphone <u>Concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition :</u> • identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe) • date et lieu de naissance • situation familiale • nationalité • adresses • profession • état de la personne • signalement (personnes disparues et corps non identifiés) • photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale (photographie du visage de face des personnes disparues et corps non identifiés) • photographies (personnes disparues et corps non identifiés)

Critères d'inscription dans ce fichier	• Les personnes mises en cause pour des crimes, délits ou contraventions de 5e classe • Les victimes de ces infractions • Les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition
Date de création	4 mai 2012
Autorité(s) compétente(s)	Le ministère de l'intérieur
Qui a accès à ce fichier ?	Personnels habilités dans le cadre d'enquêtes judiciaires ou administratives mais aussi lors des demandes d'acquisition de la nationalité française : • Les policiers • Les gendarmes • Les douanes judiciaires • Les magistrats
Durée de conservation des données	Les données concernant les personnes majeures mises en cause : • 20 ans • par dérogation, 5 ans pour certains délits, comme ceux prévus par le code de la route • par dérogation, 40 ans pour certaines infractions, comme empoisonnement, enlèvement, séquestration, prise d'otage, exploitation de la mendicité aggravée ou en bande organisée, meurtre, assassinat, etc. Les données concernant les personnes mineures mises en cause : • 5 ans pour les mineurs mis en cause • par dérogation, 10 ans pour certaines infractions comme vol avec violences, exhibition sexuelle, etc. • par dérogation, 20 ans pour d'autres infractions comme viol, torture, meurtre, assassinat, vol avec arme, etc. Les données concernant les victimes : 15 ans pour les victimes. Il y possibilité de demander l'effacement de son inscription dans le TAJ dès que l'auteur des faits a été condamné de manière définitive. Les données concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherches des causes de la mort, de blessures graves ou d'une disparition : jusqu'à ce que l'enquête ait permis de retrouver la personne disparue ou d'écarter tout suspicion de crime ou délit.
Interconnexion avec d'autres fichiers ?	Une interconnexion avec les traitements de rédaction des procédures de la police et de la gendarmerie nationales (LRPPN et LRPGN), le logiciel de rédaction des procédures des douanes judiciaires (LRPDJ) et le traitement CASSIOPEE est prévue pour l'alimentation automatique du TAJ. En outre, des interconnexions sont prévues avec des traitements utilisés pour la réalisation d'enquêtes administratives, notamment le traitement ACCReD autorisé par le décret n° 2017-1224 du 3 août 2017.
Quelle échelle ?	Nationale

Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Code de procédure pénale, articles R.40-23 à R.40-34. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6BC99B3379FA142D633EA913C49ABBB2.tplgfr22s_2?idSectionTA=LEGISCTA000025818428&cidTexte=LEGITEXT000006071154&dateTexte=20190318* - Décret n°2018-687 du 1 er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.legifrance.gouv.fr/eli/decret/2018/8/1/JUSC1815709D/jo/texte* - Décret n°2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000025803463&dateTexte=&oldAction=rechJO&categorieLien=id* - Code de procédure pénale, articles R.40-23 à R.40-34. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6BC99B3379FA142D633EA913C49ABBB2.tplgfr22s_2?idSectionTA=LEGISCTA000025818428&cidTexte=LEGITEXT000006071154&dateTexte=20190318*
Comment obtenir communication et rectification des données ?	Droit d'accès et de rectification direct auprès du : *Ministère de l'Intérieur* *Place Beauvau* *75018 Paris* Le ministère a 2 mois pour répondre. Droit d'accès et de rectification indirect : si le ministère de l'Intérieur répond négativement à la demande d'accès direct ou s'il ne donne pas de réponse à l'issue du délai de 2 mois. Doivent être communiqués à la CNIL à l'appui de la demande : -la copie d'un titre d'identité ou extrait d'acte de naissance -la copie du courrier défavorable du ministère de l'intérieur ou, à défaut de réponse de sa part dans les 2 mois, la copie du courrier de demande initiale Pour les personnes enregistrées en qualité de mise en cause, autre possibilité : adresser une requête par LRAR soit directement au procureur de la République territorialement compétent, soit au magistrat référent en charge de ce fichier pour que les données soient rectifiées / effacées / fassent l'objet d'une mention qui a pour effet de les rendre inaccessibles dans le cadre de la consultation de TAJ à des fins d'enquêtes administratives. Si le procureur de la République / magistrat référent n'ordonne pas l'effacement ou la rectification, l'intéressé peut saisir le président de la chambre de l'instruction de la cour d'appel de Paris dans un délai d'un mois à compter de l'envoi de la décision de refus.
Sources	- M. Durenton et J.P Foegle, « Fichage partout, oubli nulle-part ? Le Conseil d'Etat ouvre un boulevard au fichier Taj », Actualités droits et libertés, juillet 2014. *https://journals.openedition.org/revdh/849* - Service public, « Traitement d'antécédents judiciaires ». *https://www.service-public.fr/particuliers/vosdroits/F32727* - CNIL, « TAJ : Traitement d'Antécédents Judiciaires ». *https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires*

Nom du fichier	**TES**
Sens de l'acronyme	Titre Electronique Sécurisé
Objectif explicite	• Procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation des cartes nationales d'identité et des passeports • Prévenir et détecter leur falsification et contrefaçon *Article 1 du décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité*
Objectif implicite/ Remarques	Selon la Commission Nationale Consultative des Droits de l'Homme (CNCDH), « *derrière l'objectif affiché de simplification administrative et de lutte contre la fraude, le risque existe de créer un véritable outil de renseignement dans un contexte général d'érosion du droit à la sureté et à la liberté personne (article 2 de la DDHC de 1789). Le décret prévoit déjà que de nombreux éléments de la base d'information seront partagés par les services de renseignements dans le cadre de la lutte contre le terrorisme. Il demeure également un risque de détournement de la finalité du fichier, l'existence d'une base centrale de données biométriques pouvant en effet susciter, à l'avenir, la tentation d'en faire un outil d'identification des personnes à partir d'une trace.* » CNCDH, Déclaration « Pour la suspension du fichier dit « Titres électroniques sécurisés » », 15 décembre 2016. *https://www.cncdh.fr/fr/actualite/pour-la-suspension-du-fichier-dit-titres-electroniques-securises-tes* L'Observatoire des libertés et du numérique craint également que le fichier TES ne devienne une « *réserve d'empreintes et de photographies* », « *faisant de tout citoyen un suspect en puissance* ». (Observatoire des libertés et du numérique, Communiqué de presse du 14 novembre 2016, « Fichier TES : danger pour les libertés ». *https://www.lececil.org/node/19288)*
Contenu des données	Donnés relatives au demandeur ou au titulaire du titre : • Nom de famille, d'usage, prénoms • Date et lieu de naissance • Sexe • Couleur des yeux • Taille • Domicile ou résidence • Données relatives à la filiation • Document attestant de la qualité du représentant légal lorsque le titulaire du titre est un mineur ou un majeur placé sous tutelle • Image numérisée du visage et celle des empreintes digitales qui peuvent être légalement recueillies • Image numérisée de la signature du demandeur de la carte nationale d'identité Donnés relatives au titre : • Numéro du titre • Type du titre • Tarif du droit de timbre • Date et lieu de délivrance • Autorité de délivrance • Date d'expiration Données relatives au fabricant du titre et aux agents chargés de la délivrance du titre : nom, prénom, références de l'agent qui enregistre la demande de titre. L'image numérisée des pièces du dossier de demande de titre. ↳ *Liste exhaustive des données à l'article 2 du décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité* : *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&categorieLien=id*
Critères d'inscription dans ce fichier	Avoir demandé la délivrance ou le renouvellement d'une carte nationale d'identité ou d'un passeport

Date de création	28 octobre 2016
Autorité(s) compétente(s)	Le ministère de l'intérieur
Qui a accès à ce fichier ?	• Les agents diplomatiques et consulaires chargés de la délivrance des passeports et des cartes nationales d'identité, individuellement désignés et dûment habilités par l'ambassadeur ou le consul. • Les agents chargés de la délivrance des passeports de service au ministère de l'intérieur, individuellement désignés et dûment habilités par le ministre de l'intérieur. • Les agents des communes individuellement désignés et dûment habilités par le maire. • Pour les seuls passeports de mission, les agents des formations administratives du ministère de la défense, individuellement désignés et dûment habilités par le ministre de la défense. Accès aux données à l'exclusion de l'image numérisée des empreintes digitales : • Les agents des services de la police nationale et les militaires des unités de la gendarmerie nationale chargés des missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, individuellement désignés et dûment habilités par le directeur dont ils relèvent. • Les agents des services spécialisés du renseignement mentionnés à l'article R. 222-1 du code de la sécurité intérieure, individuellement désignés et dûment habilités par le directeur dont ils relèvent, pour les seuls besoins de la prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme. • Les agents de la direction centrale de la police judiciaire, individuellement désignés et dûment habilités par le directeur dont ils relèvent, chargés des échanges avec INTERPOL au titre de la position commune du 24 janvier 2005 susvisée et du règlement d'INTERPOL sur le traitement des données, ainsi qu'avec les autorités compétentes des Etats appliquant 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), au titre de ses articles 7, 38 et 39. *Articles 3 et 4 du décret du 28 octobre 2016*
Durée de conservation des données	• Données à caractère personnel du demandeur/titulaire du titre sont conservées dans le traitement pendant 15 ans s'il s'agit d'un passeport et 20 ans s'il s'agit d'une carte nationale d'identité. Ces durées sont respectivement de 10 ans et de 15 ans lorsque le titulaire du titre est un mineur. • Données relatives aux passeports de service et aux passeports de mission sont conservées pendant 10 ans. • Données relatives aux cartes nationales d'identité délivrées à des majeurs et périmées au 1er janvier 2014 sont conservées pendant 15 ans. Le délai court à compter de la délivrance du titre, ou, à défaut, à compter de l'enregistrement de la demande.
Interconnexion avec d'autres fichiers ?	Avec le SIS II et les données collectées par Interpol
Quelle échelle ?	Nationale et internationale avec la communication des données
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&categorieLien=id* - Délibération de la CNIL n° 2016-292 du 29 septembre 2016 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979*
Comment obtenir communication et rectification des données ?	Le droit d'accès et le droit de rectification s'exercent auprès de l'autorité de délivrance dans les conditions fixées aux *articles 39 et 40 de la loi du 6 janvier 1978 modifiées par la loi n°2018-493 du 20 juin 2018*.
Sources	- Légifrance, voir la rubrique les « Lois qui régissent ce fichier ». - CNCDH, Déclaration « Pour la suspension du fichier dit « Titres électroniques sécurisés » », 15 décembre 2016. *https://www.cncdh.fr/fr/actualite/pour-la-suspension-du-fichier-dit-titres-electroniques-securises-tes* - Le site de l'Observatoire des libertés et du numérique, Communiqué de presse du 14 novembre 2016, « Fichier TES : danger pour les libertés ». *https://www.lececil.org/node/19288*

Nom du fichier	**VISABIO**
Sens de l'acronyme	Visa Biométrique
Objectif explicite	• Mieux garantir le droit au séjour des personnes en situation régulière et de lutter contre l'entrée et le séjour irréguliers des étrangers en France, en prévenant les fraudes documentaires et les usurpations d'identité. • Permettre l'instruction des demandes de visas en procédant notamment à l'échange d'informations, d'une part, avec des autorités nationales, d'autre part, avec les autorités des Etats Schengen au travers du système d'information sur les visas (VIS) pour les données biométriques se rapportant aux visas court séjour délivrés par les autorités françaises. • Lors de la demande de visa : déterminer si une personne a déjà sollicité un visa sous une autre identité. • Lors du passage de la frontière : vérifier l'authenticité du visa et l'identité de son détenteur. • Lors des contrôles d'identité sur le territoire national : vérifier l'identité de la personne, l'authenticité du visa et la régularité de son séjour en France. • Faciliter l'identification des étrangers en situation irrégulière en vue de leur éloignement. • Faciliter la détermination et la vérification de l'identité d'un étranger qui se déclare mineur privé temporairement ou définitivement de la protection de sa famille. *Article R. 611-8 du CESEDA*
Objectif implicite/ Remarques	Contrôle accru des demandeurs de visa par le biais de l'utilisation des données biométriques, lutte contre la fraude.
Contenu des données	• Les images numérisées de la photographie et des empreintes digitales des dix doigts des demandeurs de visas (sauf des mineurs de moins de douze ans), collectées par les chancelleries consulaires et les consulats français équipés du dispositif requis. • Les données contenues dans le RMV 2, lors de la demande et de la délivrance d'un visa. • Les données recueillies ultérieurement lors des entrées et sorties du détenteur de visa : date de première entrée, date de dernière entrée et date de sortie. *Article R. 611-9 du CESEDA*
Critères d'inscription dans ce fichier	Déposer une demande de visa
Date de création	03 novembre 2007
Autorité(s) compétente(s)	Le ministère de l'Europe et des affaires étrangères et le ministère de l'intérieur sont co-responsables du système d'information sur les visas
Qui a accès à ce fichier ?	• Les agents du ministère de l'Europe et des affaires étrangères et du ministère de l'intérieur • Les agents de préfecture • Les agents chargés du contrôle aux frontières • Les agents du ministère de l'intérieur • Certains officiers de police judiciaire des services de la police et de la gendarmerie nationale • Les agents de douane • Les agents de l'OFII chargés des procédures d'admission au séjour • les agents chargés de la mise en œuvre de la protection de l'enfance • Les agents de service de la police nationale • Les militaires des unités de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme • Les agents des services spécialisés du renseignement
Durée de conservation des données	Cinq ans à compter de l'enregistrement de la demande de visa

Interconnexion avec d'autres fichiers ?	Il permet des échanges d'informations, d'une part entre autorités nationales (police, préfecture, directions départementales de la Police des Frontières, etc …), et d'autre part, avec les autorités des Etats Schengen au travers du système d'information sur les visas (VIS) II. *Article R. 611-8 du CESEDA*
Quelle échelle ?	Nationale et internationale avec la communication des données
Lois qui régissent ce fichier	- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. *https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee* - Code de l'entrée et du séjour des étrangers et du droit d'asile, articles R. 611-8 à R. 611-15 du CESEDA. *https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006163296&cidTexte=LEGITEXT000006070158&dateTexte=20110426* - Décret n° 2019-57 du 30 janvier 2019 relatif aux modalités d'évaluation des personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille et autorisant la création d'un traitement de données à caractère personnel relatif à ces personnes. *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=973F0ED59C3ECC4D9FC45EA2E134F0A0.tplgfr32s_2?cidTexte=JORFTEXT000038074279&dateTexte=20190201* - Décret n°2013-147 du 18 février 2013 relatif à l'application de gestion des dossiers de ressortissants étrangers en France et au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027088465&categorieLien=id* - Décret n°2007-1560 du 2 novembre 2007 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa pris pour l'application de l'article L. 611-6 du code de l'entrée et du séjour des étrangers et du droit d'asile et modifiant la partie réglementaire de ce code. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000825481&dateTexte=* - Délibération n° 2007-195 du 10 juillet 2007 portant avis sur le projet de décret pris pour l'application de l'article L. 611-6 du code de l'entrée et du séjour des étrangers et du droit d'asile portant création d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa et modifiant la partie réglementaire de ce même code. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000825669&categorieLien=id*
Comment obtenir communication et rectification des données ?	Droits d'accès et de rectification (*articles 39 et 40 de la loi n° 78-17 du 6 janvier 1978 modifiés par la loi n°2018-493 du 20 juin 2018*) : ⇨ auprès du service où la délivrance du visa a été sollicitée. ⇨ ou par écrit auprès du ministère de l'intérieur (sous-direction des visas) ou du ministère de l'Europe et des affaires étrangères (direction des Français à l'étranger et de l'administration consulaire). Pas de droit d'opposition (*article 38 de la loi du 6 janvier 1978 susmentionnée modifié par la loi n°2004-801 du 6 août 2004*).
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - La Cimade, Rapport d'observation, « Visa refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas », juillet 2010. *https://www.lacimade.org/wp-content/uploads/2015/12/Rapport_VisaRefuse_PremierePartie_definitif.pdf*

Nom du fichier	**EURODAC**
Sens de l'acronyme	EU Biometric Data Base
Objectif explicite	Eurodac est un système d'information à grande échelle contenant les empreintes digitales des demandeurs d'asile et de protection subsidiaire et immigrants illégaux se trouvant sur le territoire de l'UE. • Contribuer à l'application efficace de la convention de Dublin III. Elle permet de déterminer le pays de l'UE responsable de l'examen d'une demande d'asile ou de protection subsidiaire. Lorsqu'un pays participant envoie un jeu d'empreintes à Eurodac, il sait immédiatement si celles-ci correspondent à des empreintes qui se trouvent déjà dans la base de données. En cas de concordance : le pays peut choisir de renvoyer la personne dans le premier pays où elle est arrivée ou dans lequel elle a présenté une demande d'asile ou de protection subsidiaire. En l'absence de concordance : c'est le pays qui a soumis les empreintes qui traite la demande. • Permettre aux autorités répressives de consulter la base Eurodac à des fins d'investigation, de détection et de prévention d'actes terroristes ou autres infractions pénales graves. Site de la CNIL : *https://www.cnil.fr/fr/systeme-dinformation-eurodac*
Objectif implicite/ Remarques	Empêcher la pratique de « l'asylum shopping », c'est-à-dire le dépôt de différentes demandes d'asile dans plusieurs Etats de l'UE. (Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013 *https://hal.archives-ouvertes.fr/hal-01614132/document)* *Remarque* : dans le cadre d'un projet de refonte du système « Dublin », la Commission européenne propose d'adapter et de réformer Eurodac et d'en élargir l'objet, afin de faciliter les retours et de lutter contre la migration irrégulière. Dans une communication du 4 mai 2016 (Doc.COM (2016) 272 final, 4 mai 2016), la Commission européenne propose ainsi une nouvelle extension du champ d'application du règlement « Eurodac », afin de permettre aux États membres de stocker et de rechercher des données relatives aux ressortissants de pays tiers ou apatrides, ne relevant pas de la protection internationale et en situation irrégulière dans l'Union, de sorte qu'ils puissent être identifiés à des fins de retour ou de réadmission. Portée en même temps que le projet de révision du règlement « Dublin », cette proposition devrait également permettre aux États membres, « dans le plein respect des règles en matière de protection des données », de stocker davantage de données à caractère personnel, telles que le nom, la date de naissance, la nationalité, des éléments d'identification ou des documents de voyage, et l'image faciale. Le projet de la nouvelle base de données se rapproche de plus en plus d'un très ancien projet : celui de disposer d'une base de données unique dans le domaine asile/immigration. Le projet prévoit également d'abaisser l'âge de la prise d'empreintes de 14 à 6 ans. *(Dictionnaire permanent, droit des étrangers, « Fichiers informatiques », ELnet)*
Contenu des données	Outre les empreintes digitales, les données transmises par les pays de l'UE contiennent : • Le pays de l'UE d'origine • Le sexe de la personne • Le lieu et la date de la demande d'asile ou de protection subsidiaire ou le lieu et la date où l'intéressé a été appréhendé • Le numéro de référence • La date à laquelle les empreintes ont été relevées • La date à laquelle les données ont été transmises à l'unité centrale Les données sont relevées pour toute personne de plus de 14 ans et sont envoyées à l'unité centrale par des points d'accès nationaux. Dans certaines conditions, les données suivantes peuvent également être conservées dans l'unité centrale du traitement : • La date d'arrivée de la personne concernée à la date d'un transfert réussi lorsqu'une requête à des fins de reprise a été acceptée, et que par conséquent la personne arrive dans l'Etat membre à la suite de ce transfert • La date à laquelle la personne a quitté le territoire ou en a été éloignée ; soit dans le cas où cette personne a simplement quitté le territoire de l'UE, soit dans le cas où

	cette personne a quitté le territoire en exécution d'une décision de retour ou d'une mesure d'éloignement prononcée à la suite du retrait ou du rejet d'une demande de protection internationale • La date à laquelle la décision d'examiner la demande a été prise, lorsqu'un pays membre décide tout de même d'examiner une demande de protection internationale alors que cette obligation ne lui incombe pas en vertu de la réglementation applicable en matière d'asile
Critères d'inscription dans ce fichier	• Avoir demandé l'asile dans un des Etats de l'Espace Schengen • Avoir été appréhendé lors du franchissement irrégulier d'une frontière extérieure de l'UE ⇨ *Les empreintes des personnes âgées d'au moins 14 ans sont relevées.*
Date de création	Règlement 11 décembre 2000
Autorité(s) compétente(s)	Au niveau européen : le système est composé d'une unité centrale équipé d'un système informatisé de reconnaissance des empreintes digitales. Il est géré opérationnellement au sein de l'agence EU-Lisa qui gère la base de données centrale pour le compte des Etats-membres et effectue des statistiques (*article 8 du Règlement (UE) n°603/2013 du Parlement européen et du Conseil du 26 juin 2013*). Au niveau national : Le ministère de l'Intérieur français est responsable des données qu'il introduit dans le système. Les services français chargés du recueil des demandes d'asile, à savoir les services préfectoraux compétents, peuvent procéder à une inscription. Chaque Etat membre désigne et notifie à l'agence EU-Lisa et à la Commission les unités responsables (*article 27 du Règlement (UE) précité*). Liste par pays : *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2015.237.01.0001.01.FRA&toc=OJ:C:2015:237:TOC*
Qui a accès à ce fichier ?	Chaque Etat membre désigne et notifie à l'agence EU-Lisa (Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice) et à la Commission européenne la liste des autorités nationales compétentes pour consulter EURODAC. La CNIL est également destinataire et dépositaire de cette liste. Pour la France, cette liste a été publiée au Journal officiel de l'Union européenne du 20 juillet 2015 (*https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2015.237.01.0001.01.FRA&toc=OJ:C:2015:237:TOC*) : *Ministère de l'intérieur, Direction générale des étrangers en France (DGEF), Service de l'asile* *Département de l'asile à la frontière et de l'admission au séjour* *Place Beauvau* *75800 Paris Cedex 08* Depuis le 20 juillet 2015 (*Règlement n°603/2013*), les autorités de police désignées des États membres et l'Office européen de police (Europol) peuvent demander la comparaison de données dactyloscopiques avec celles conservées dans le système central à des fins répressives (dans le cadre d'une procédure pénale particulière).
Durée de conservation des données	• Les données enregistrées à l'occasion de l'enregistrement d'une demande d'asile ou de protection subsidiaire : sont conservées dans le système central pendant dix ans à compter de la date du relevé des empreintes. Passé ce délai, les données sont automatiquement effacées du système central. Les données concernant un demandeur qui se verrait accorder l'asile sont masquées à compter de l'accord de la protection puis supprimées à l'issue du délai de 10 ans. Les données des personnes ayant acquis la nationalité d'un Etat membre de l'Union européenne font également l'objet d'un effacement automatique. • Les données relatives aux ressortissants étrangers appréhendés à l'occasion du franchissement illégal d'une frontière : sont conservées dix-huit mois dans l'unité centrale du traitement. • Les données relatives aux ressortissants étrangers se trouvant illégalement sur le territoire de l'UE : ne sont pas conservées dans le traitement. Elles ne sont utilisées qu'à des fins de comparaison immédiate.

Interconnexion avec d'autres fichiers ?	La Commission européenne, dans sa proposition de Règlement relative à la refonte d'Eurodac, propose la constitution d'un groupe d'experts sur les systèmes d'information et l'interopérabilité afin de déterminer si une interopérabilité future avec le SIS et le VIS est nécessaire et proportionnée. *Proposition de Règlement du Parlement européen et du Conseil 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 de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte).* *http://ec.europa.eu/transparency/regdoc/rep/1/2016/FR/1-2016-272-FR-F1-1.PDF*
Quelle échelle ?	Européenne
Lois qui régissent ce fichier	- Règlement (UE) N°603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac (Applicable à partir du 20 juillet 2015). *https://www.gisti.org/spip.php?article3251* - Règlement (CE) N°407/2002 du Conseil du 28 février 2002 fixant certaines modalités d'application du règlement (CE) no 2725/2000 concernant la création du système « Eurodac », texte abrogé. *https://www.gisti.org/spip.php?article1589* - Règlement 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, texte abrogé. *https://www.gisti.org/spip.php?article1588*
Comment obtenir communication et rectification des données ?	Toute personne peut accéder aux données la concernant, ainsi qu'à l'identité de l'Etat membre ayant transmis ces données au système centrale par l'intermédiaire d'un Etat membre. La demande d'accès doit être adressée au *Service de l'Asile rattaché à la DGEF du ministère de l'intérieur (Place Beauvau, 75800 Paris Cedex 08)*. Celui-ci prendra attache avec l'administration concernée afin de préparer la procédure d'interrogation et de communication, le cas échéant, des données. La procédure d'interrogation nécessitera notamment la présence du demandeur afin qu'il puisse présenter ses empreintes à une borne Eurodac (en préfecture par exemple). En cas de concordance avec une fiche, les données contenues dans le fichier seront transmises à la personne. De même, les demandes de rectification doivent être effectuées auprès de l'Etat membre qui a transmis les données.
Sources	- Le site du GISTI relatif à Dublin et EURODAC. *https://www.gisti.org/spip.php?rubrique392* - Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013. *https://hal.archives-ouvertes.fr/hal-01614132/document* - Dictionnaire juridique de droit des étrangers, Etude « fichiers informatiques ». - CNIL, « Système d'information EURODAC ». *https://www.cnil.fr/fr/systeme-dinformation-eurodac*

Nom du fichier	**SIS II**
Sens de l'acronyme	Système d'Information Schengen II
Objectif explicite	• Permettre aux Etats membres de l'espace Schengen de **mettre en place une politique commune de contrôle des entrées dans l'espace Schengen** et, ainsi, de faciliter la libre circulation de leurs ressortissants tout en préservant l'ordre et la sécurité publics. • Assurer un niveau de sécurité élevé au sein des États Schengen en l'absence de contrôles aux frontières intérieures, en permettant aux autorités nationales compétentes, comme les forces de police et les gardes-frontières, de **saisir et de consulter des signalements concernant des personnes ou des objets**. Site de la CNIL : *https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii*
Objectif implicite/ Remarques	Le fichier SIS II, à l'instar du VIS et d'EURODAC, a pour visée de lutter entre autre contre l'immigration irrégulière, la fraude, les fausses identités. Les normes qui ont modifié les différents fichiers précités au cours de leur histoire ont petit à petit pris un tournant de plus en plus sécuritaire et ont affiché ouvertement une lutte contre l'immigration clandestine. Il y a un glissement du passage du fichier SIS comme fichier d'identification à un fichier d'intelligence, un fichier d'enquête policière. (Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013. *https://hal.archives-ouvertes.fr/hal-01614132/document*)
Contenu des données	Structure du SIS II : • le système central = le **C-SIS II central**, contient la base de données SIS II • le système national dans chaque Etat membre = le **N-SIS II** • une infrastructure de communication entre le système central et les systèmes nationaux Le système d'information Schengen de deuxième génération (« SIS II ») est une grande base de données qui contient des informations sur des **personnes recherchées ou disparues, des personnes sous surveillance policière et des personnes non ressortissantes d'un État membre de l'espace Schengen auxquelles l'entrée sur le territoire Schengen est interdite**, ainsi que des informations sur des véhicules et objets volés ou disparus, comme des documents d'identité, des certificats d'immatriculation de véhicules et des plaques d'immatriculation de véhicules. Données concernant les personnes signalées dans le C-SIS II : • les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, éventuellement enregistrés séparément • les signes physiques particuliers, objectifs et inaltérables • le lieu et la date de naissance • le sexe • les photographie • les empreintes digitales • la ou les nationalités • l'indication que la personne concernée est armée, violente ou en fuite • le motif du signalement • l'autorité signalante • une référence à la décision qui est à l'origine du signalement • les mesures à prendre • le(s) lien(s) vers d'autres signalements introduits dans le SIS II conformément à l'article 52 • le type d'infraction Données dans le N-SIS II : • l'état civil (noms, prénoms et alias, date et lieu de naissance), le sexe et la nationalité • les signes physiques particuliers, objectifs et inaltérables, et l'indication que la personne est armée ou violente • le motif du signalement • la conduite à tenir en cas de découverte

Critères d'inscription dans ce fichier	Appartenir à l'une des catégories suivantes : • Des personnes recherchées ou disparues • Des personnes sous surveillance policière et des personnes non ressortissantes d'un État membre de l'espace Schengen auxquelles l'entrée sur le territoire Schengen est interdite • Des informations sur des véhicules et objets volés ou disparus, comme des documents d'identité, des certificats d'immatriculation de véhicules et des plaques d'immatriculation de véhicules
Date de création	20 décembre 2006
Autorité(s) compétente(s)	La direction générale de la police nationale du ministre de l'intérieur
Qui a accès à ce fichier ?	Au niveau français : • Les fonctionnaires et agents de l'Etat du bureau SIRENE français (Supplément d'Information Requis à l'Entrée dans un Etat membre : bureau qui gère la partie nationale N-SIS et destinataire de demandes de signalements effectués en France) • Les autorités judiciaires • Les fonctionnaires de la police nationale et les militaires de la gendarmerie nationale dûment habilités qui agissent dans le cadre de leur mission générale de police administrative et de police judiciaire • Les agents des préfectures et des services de l'administration centrale du ministère de l'intérieur compétents en matière d'entrée, de séjour et d'éloignement des étrangers et de recherche des personnes, majeures ou mineures, disparues, pour les seules consultations relevant de leurs attributions • Les agents des services du ministère des affaires étrangères chargés de la délivrance des visas, des consulats et sections consulaires d'ambassades, pour les seuls renseignements concernant des étrangers signalés aux fins de non-admission dans l'espace Schengen • Les agents des douanes, pour les informations concernant les étrangers non admissibles ; pour certaines catégories de signalements, les agents des douanes sont informés de l'existence d'un signalement et doivent saisir l'officier de police judiciaire le plus proche • Les autorités et services homologués des autres Etats membres de l'espace Schengen Dans les autres Etats membres de l'UE : • Les autorités nationales compétentes légalement désignées à cette fin • Europol • Les membres nationaux d'Eurojust et leurs assistants (Eurojust est l'agence européenne chargée de renforcer la coopération judiciaire entre les Etats membres, pour les poursuites relatives à la criminalité organisée)
Durée de conservation des données	Les informations sont conservées trois ans. Passé ce délai, le service chargé du fichier examine si l'inscription doit être prolongée ou non. Les inscriptions concernant des objets (véhicules recherchés, armes, pièces d'identité volées, etc.) sont conservées cinq ans ou dix ans selon les cas.
Interconnexion avec d'autres fichiers ?	Les signalements effectués par l'Etat français dans le N-SIS II découlent des signalements introduits dans le Fichier des personnes recherchées (FPR), le fichier des objets volés et signalés (FOVeS), le fichier des titres électroniques sécurisés (TES) et DOCVERIF (fichier ayant pour objectif de lutter contre l'utilisation indue, la falsification ou la contrefaçon de documents d'identité).
Quelle échelle ?	Européenne
Lois qui régissent ce fichier	- 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. *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32018R1860* - 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. *https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32018R1861* - Règlement 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) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission. *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1862&from=EN* - Décision du Conseil du 7 mars 2013 fixant la date d'application du règlement (CE) n° 1987/2006 du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).*https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2013.087.01.0010.01.FRA&toc=OJ:L:2013:087:TOC*

	- 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). *https://eur-lex.europa.eu/eli/dec/2007/533/oj* - Règlement (CE) nº 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). *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32006R1987* - Règlement (CE) No 1986/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II). *https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32006R1986* - Décision de la Commission du 4 mai 2010 établissant un plan de sécurité pour le SIS II central et l'infrastructure de communication (2010/261/UE). *https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32010D0261* - Décision d'exécution (UE) 2016/ 1209 de la Commission du 12 juillet 2016 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. *https://eur-lex.europa.eu/legal-content/FR/TXT/ELI/?eliuri=eli:dec_impl:2016:1209:oj* - Liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d'information Schengen de deuxième génération. *http://securibase.com/securibase/public/fiche/21185/23776* - Code de la sécurité intérieure, articles R. 231-1 à R. 231-16. *https://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000033825160&idSectionTA=LEGISCTA000028287315&cidTexte=LEGITEXT000025503132&dateTexte=20190320* - Décret n° 2016-1956 du 28 décembre 2016 relatif à la partie nationale du système d'information Schengen de deuxième génération (N-SIS II). *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033736248&categorieLien=id* - CNIL, Délibération n°95-047 du 25 avril 1995 relative au système informatique de la partie nationale du système d'information Schengen mis en œuvre par le ministère de l'intérieur. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653524*
Comment obtenir communication et rectification des données ?	Le droit d'accès au N-SIS II s'exerce auprès de la CNIL, sauf pour certaines catégories de signalements pour lesquels il faut solliciter, en application de dispositions réglementaires, directement la communication des données auprès du ministère de l'intérieur (comme pour un mineur faisant l'objet d'une opposition à sortie du territoire sans l'accord des deux parents ou signalé comme fugueur …). Demande adressée à la CNIL : impérativement accompagnée d'une copie d'un titre d'identité, auquel peut être joint tout autre document utile à l'instruction de la demande (copie de la décision de refus de visa Schengen, décision d'abrogation d'un arrêté préfectoral d'expulsion...) ⇨ Un magistrat de la Commission en charge du droit d'accès indirect va procéder à la vérification et, si nécessaire, à la rectification du fichier ⇨ Si la personne est déjà signalée par une autre Etat membre, la CNIL sollicite la coopération de l'autorité de contrôle de cet Etat afin de vérifier le bien-fondé et l'exactitude du signalement ⇨ Au terme de la vérification, un courrier sera adressé à l'intéressé pour lui faire part du résultat. Si la vérification permet de constater que les données relèvent du droit d'accès direct, la personne en sera tenue informée. Si les données relèvent du droit d'accès direct, s'adresser directement au ministère de l'intérieur (délai moyen de traitement des demandes : 2 mois) : *Direction Centrale de la Police Judiciaire* *Place Beauvau* *F-75008 Paris*
Sources	- CNIL, « SIS II : Système d'information Schengen II ». https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii - Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013. *https://hal.archives-ouvertes.fr/hal-01614132/document*

Nom du fichier	**VIS**
Sens de l'acronyme	Visa Information System
Objectif explicite	Selon la CNIL, le Système d'information sur les visas (VIS) est utilisé pour l'examen des demandes de visas de court séjour et des décisions de refus, de prorogation, d'annulation ou de retrait de visa, ainsi que les vérifications des visas et les vérifications et identifications des demandeurs et des détenteurs de visa. Objectif d'améliorer la mise en œuvre ⇨ de la politique commune en matière de visas ⇨ de la coopération consulaire ⇨ des consultations des autorités centrales chargées des visas, en facilitant l'échange de données entre les Etats membres sur les demandes de visas et les décisions qui y sont relatives Dans le but de ⇨ simplifier la procédure de demande de visa ⇨ prévenir les demandes multiples de visas ⇨ faciliter la lutte contre la fraude ⇨ faciliter les contrôles aux points de passage aux frontières extérieures et sur le territoire national ⇨ contribuer à l'identification de toute personne qui ne remplit pas les conditions d'entrée / de présence / de séjour sur le territoire national ⇨ faciliter l'application du règlement « Dublin III » ⇨ prévenir les menaces pesant sur la sécurité intérieure des pays de l'UE *Article 2 du Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les Etats membres sur les visas de court séjour (règlement VIS). https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32008R0767*
Objectif implicite/ Remarques	• Lutter contre le « visa shopping », c'est-à-dire éviter que les ressortissants d'Etats tiers fassent plusieurs demandes de visa simultanées auprès de plusieurs services consulaires. (Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013. *https://hal.archives-ouvertes.fr/hal-01614132/document*) • Permettre une identification des personnes restées sur le territoire européen au-delà de la durée de validité de leur visa et faciliter leur expulsion. (La Cimade, Rapport d'observation : « Visa Refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas », juillet 2010. *https://www.lacimade.org/wp-content/uploads/2015/12/Rapport_VisaRefuse_PremierePartie_definitif.pdf*)
Contenu des données	• Les données alphanumériques sur le demandeur et sur les visas demandés, délivrés, refusés, annulés, retirés ou prorogés • La photographie du demandeur • Les empreintes digitales du demandeur • Les liens avec les demandes de visa précédentes et avec les dossiers de demande des personnes qui voyagent ensemble. *Article 5 du Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008.*

Critères d'inscription dans ce fichier	• Lorsqu'une demande est jugée recevable conformément au code des visas, l'autorité chargée des visas crée le dossier de demande en saisissant dans le VIS un ensemble de données énoncées dans le règlement, notamment le numéro de la demande, l'autorité à laquelle la demande est présentée, la photographie et les empreintes digitales du demandeur... ↳ *Liste exhaustive des données à l'article 9 du Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32008R0767* • Lorsqu'une décision a été prise de délivrer un visa, l'autorité chargée des visas ajoute les autres données pertinentes, notamment le type de visa, le territoire sur lequel le titulaire du visa est autorisé à voyager, la durée de validité, le nombre d'entrées autorisées par le visa sur le territoire et la durée du séjour autorisé par le visa. ↳ *Liste exhaustive des données à l'article 10 du règlement précité* • Dans le cas où l'autorité chargée des visas représentant un autre pays de l'UE interrompt l'examen d'une demande de visa, elle ajoute d'autres données, notamment le nom et la localisation de l'autorité ayant interrompu l'examen de la demande de visa ou le lieu et la date de la décision d'interrompre l'examen. ↳ *Liste exhaustive des données à l'article 11 du règlement précité* • Lorsque la décision a été prise de refus un visa, l'autorité chargée des visas ajoute d'autres données, notamment les motifs de refus. ↳ *Liste exhaustive des données à l'article 12 du règlement précité* • Lorsque la décision a été prise d'annuler un visa / de retirer un visa / de réduire la durée de validité d'un visa, l'autorité chargée des visas ajoute d'autres données, notamment le lieu / la date / les motifs de cette décision. ↳ *Liste exhaustive des données à l'article 13 du règlement précité* • Lorsque la décision de proroger le visa a été prise, l'autorité chargée des visas ajoute d'autres données, notamment la période de prorogation de la durée autorisée, les motifs de la prorogation... ↳ *Liste exhaustive des données à l'article 14 du règlement précité*
Date de création	8 juin 2004
Autorité(s) compétente(s)	Le ministère de l'Europe et des affaires étrangères et le ministère de l'intérieur sont co-responsables du système d'information sur les visas
Qui a accès à ce fichier ?	*Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS)* : • Autorités compétentes chargées des visas – le personnel des ambassades et des consulats – aux fins de l'examen des demandes, avec accès au dossier de demande en cas de présence d'une donnée recherchée (*article 15*) • Autorités centrales chargées des visas pour les demandes de consultation, avec saisine du VIS central, qui transmet la demande aux États concernés (*article 16*) ; elles peuvent consulter un ensemble de données pour établir des statistiques, sans identification du demandeur (*article 17*) • Autorités centrales chargées des contrôles aux points de passage aux frontières extérieures Schengen pour vérifier l'identité du titulaire de visa, recherches effectuées avec le numéro de la vignette visa en combinaison avec les empreintes digitales (*article 18*) ; en cas de doute sur l'identité du titulaire du visa ou l'authenticité de celui-ci, le personnel pourra consulter l'ensemble des données (*article 20*) • Autorités centrales chargées du contrôle sur le territoire (*article 19*), pour vérifier l'identité du titulaire, l'authenticité du visa ou si les conditions d'entrée/de séjour sont remplies : même règle que ci-dessus (*article 20*) • Autorités compétentes en matière d'asile : elles effectuent des recherches à l'aide des empreintes digitales pour deux motifs la consultation du VIS étant autorisée pour ces autorités (*article 21*) : dans le seul but de déterminer l'État responsable de l'examen de la demande d'asile (Dublin II) ou d'examiner une demande d'asile (la procédure est la même dans les deux cas) • Autorité nationale désignée comme responsable du traitement au sens de l'article 2, point d) de la directive 95/46/CE du Parlement européen et du Conseil et ayant la responsabilité centrale du traitement des données par l'État membre concerné • Europol en consultation dans les limites de ses missions (*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 Etats 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, JOUE L 218/129, 13 août 2008)*

Durée de conservation des données	Chaque dossier de demande est enregistré dans le VIS pour une durée maximale de cinq ans. Seul le pays responsable est autorisé à modifier ou à supprimer les données qu'il a transmises au système VIS.
Interconnexion avec d'autres fichiers ?	Le VIS est interconnecté dans la pratique avec des fichiers nationaux. En France, il s'agit de VISABIO et de RMV2.
Quelle échelle ?	Européenne
Lois qui régissent ce fichier	- Règlement (CE) n°810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas. *https://www.gisti.org/spip.php?article1418* - Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (Règlement VIS). *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008R0767&from=FR* - 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). http://cdre.eu/75-documentation-en-ligne/cooperation-policiere/legislation/240-decision-2008-633-jai-du-conseil-du-23-juin-2008-concernant-l-acces-en-consultation-au-systeme-d-information-sur-les-visas-vis-par-les-autorites-designees-des-etats-membres-et-par-l-office-eu - Décision du Conseil 2004/512/CE du 8 juin 2004 établissant le système d'information sur les visas (VIS). *https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004D0512*
Comment obtenir communication et rectification des données ?	Droits d'accès et de rectification (*articles 39 et 40 de la loi n° 78-17 du 6 janvier 1978 modifiés par la loi n°2018-493 du 20 juin 2018*) : • auprès du service où la délivrance du visa a été sollicitée • ou par écrit auprès du ministère de l'intérieur (sous-direction des visas) ou du ministère de l'Europe et des affaires étrangères (direction des Français à l'étranger et de l'administration consulaire)
Sources	- Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, pp. 183 - 221, 2013. *https://hal.archives-ouvertes.fr/hal-01614132/document* - CNIL, « Système d'information sur les visas (SIV) - Visa information system (VIS) ». *https://www.cnil.fr/fr/systeme-dinformation-sur-les-visas-siv-visa-information-system-vis* - La Cimade, Rapport d'observation : « Visa Refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas », juillet 2010. *https://www.lacimade.org/wp-content/uploads/2015/12/Rapport_VisaRefuse_PremierePartie_definitif.pdf*

Nom du fichier	**API-PNR**
Sens de l'acronyme	Advance Passenger Information - Passenger name record (Renseignements préalables sur les voyageurs - Dossier Passager)
Objectif explicite	Selon la CNIL : « Le « système API-PNR France » porte sur les données de réservation (« Passenger Name Record », dites PNR) et les données d'enregistrement et d'embarquement (« Advance Passenger Information », dites API) de tous les passagers aériens. Il permettra d'effectuer un **rapprochement entre les données collectées et d'autres fichiers de police judiciaire et administrative, relatifs à des personnes ou des objets recherchés ou surveillé**s. » • Prévention et constatation des actes de terrorisme • Prévention et constatation des infractions pour lesquelles un mandat d'arrêt européen peut être exécuté • Prévention et constatation des atteintes aux intérêts fondamentaux de la Nation • Rassemblement des preuves de ces infractions et de ces atteintes ainsi que rechercher de leurs auteurs
Objectif implicite/ Remarques	Le fichier API-PNR s'inscrit dans une logique de police globale de lutte contre le terrorisme.
Contenu des données	• Les données API (Advanced passenger informations ou renseignements préalables sur les voyageurs), dites d'enregistrement et d'embarquement : ⇨ présentes dans les systèmes d'information d'enregistrement et d'embarquement des compagnies aériennes ou des plateformes aéroportuaires ⇨ informations liées à l'enregistrement des passagers provenant du passeport ou d'un autre document de voyage (nationalité, nom...) ⇨ informations générales concernant le vol (date du vol, nombre total de personnes transportées...). • Les données PNR (Passenger Name Record ou dossier passager), dites de réservation : ⇨ informations fournie par les voyageurs au stade de la réservation commerciale et contenues dans les dossiers créés par les compagnies aériennes pour chaque vol ⇨ permettent d'identifier chaque passager et d'avoir accès à tous les renseignements concernant son voyage (vols d'aller et de retour, correspondances éventuelles, moyens de paiement utilisés, services particuliers souhaités à bord, etc.) ↳ *Liste exhaustive des données à l'article R. 232-14 du code de la sécurité intérieure*
Critères d'inscription dans ce fichier	Etre un passager aérien
Date de création	26 septembre 2014
Autorité(s) compétente(s)	Ce fichier est mis en œuvre par les ministres de l'intérieur et de la défense, ainsi que par les ministères chargés des transports et des douanes
Qui a accès à ce fichier ?	Seuls les personnels affectés au sein de l'UIP (Unité d'informations des passagers : service interministériel chargé de collecter les données relatives aux passagers aériens et de les transmettre aux services compétents -police/gendarmerie/renseignement) auront directement accès aux données à caractère personnel. Sont destinataires des données enregistrées dans le traitement, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître, les services qui participent aux finalités assignées au traitement, prévus aux dispositions de l'article R. 232-15 du code de la sécurité intérieure. Ce sont notamment les services spécialisés de renseignement, les services à compétence judiciaire, les services à compétence administrative ainsi que les services ayant des compétences spécialisées en matière aéroportuaire. Les destinataires n'ont pas tous accès aux mêmes requêtes et aux mêmes modalités d'exploitation des données. Ainsi, une distinction est réalisée entre les agents des services habilités à formuler des requêtes auprès de l'UIP et à être destinataires des réponses correspondantes et ceux ne pouvant formuler aucune requête mais étant habilités à recevoir communication de certaines données à des fins opérationnelles (intervention sur les plateformes aéroportuaires). ⇨ *Liste exhaustive des destinataires aux articles R. 232-15 et R. 232-16 du code de la sécurité intérieure*.

Durée de conservation des données	Les données personnelles et les informations enregistrées sont conservées cinq ans à compter de leur réception dans le système. À l'expiration d'un délai de six mois, les données susceptibles de révéler directement l'identité des passagers sont conservées mais ne peuvent être communiquées aux services demandeurs que sur demande motivée et après autorisation expresse du directeur de l'UIP. ↳ *Liste exhaustive de ces données à l'article R. 232-20, II du code de la sécurité intérieure*.
Interconnexion avec d'autres fichiers ?	Avec les fichiers FPR, SIS II, le FOVeS (fichier des objets et véhicules signalés), le SILCF, le fichier des documents de voyage volés et perdus d'Interpol.
Quelle échelle ?	Nationale et internationale
Lois qui régissent ce fichier	- Directive 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. *https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L0681* - Articles R. 232-12 à R. 232-22 du code de la sécurité intérieure. *https://www.legifrance.gouv.fr/affichCode.do;jsessionid=6BF3B376AACE10C3721CFF60E00D2803.tplgfr31s_1?idSectionTA=LEGISCTA000029507135&cidTexte=LEGITEXT000025503132&dateTexte=20190320* - Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire). *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037301107&categorieLien=id* - Décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP). *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029953824&categorieLien=id* - Décret n° 2014-1095 du 26 septembre 2014 portant création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure. *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029504412* - Délibération n° 2014-308 du 17 juillet 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000029507988* - Délibération n° 2015-230 du 9 juillet 2015 portant avis sur un projet de décret portant modification des articles 5 du décret n° 2010-569 du 28 mai 2010 et R. 232-14 et R. 232-15 du code de la sécurité intérieure. *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000031357354*
Comment obtenir communication et rectification des données ?	Droits d'accès et de rectification (*articles 39 et 40 de la loi n° 78-17 du 6 janvier 1978 modifiés par la loi n°2018-493 du 20 juin 2018*) : • directement auprès du directeur de l'Unité Information Passagers ou de son adjoint (*UIP, 11 rue des Deux-Communes, 93558 Montreuil Cedex*) • par exception, indirectement auprès de la CNIL : - pour les mentions "connu" ou inconnu" dans les autres fichiers (FPR, SIS II, Foves, SILCF, fichier des documents de voyage volés et perdus d'Interpol) - pour les résultats des requêtes formulées par les unités et services Pas de droit d'opposition (*article 38 de la loi du 6 janvier 1978 susmentionnée modifié par la loi n°2004-801 du 6 août 2004*)
Sources	- Légifrance, voir ci-dessus les « Lois qui régissent ce fichier ». - CNIL, « Le « système API-PNR France ». *https://www.cnil.fr/fr/le-systeme-api-pnr-France*

Nom du fichier	**EUROPOL**
Sens de l'acronyme	European Police Office (Office européen de police)
Objectif explicite	Europol est une organisation intergouvernementale destinée à faciliter la coopération policière européenne. ⇨ *composition* : regroupe les services de police et les douanes des Etats membres. Chaque Etat-membre met en place une unité nationale (au sein de laquelle au moins un officier de liaison est désigné) constituant l'organe de liaison entre Europol et les autorités compétentes de l'Etat membre. ⇨ *mission* : faciliter l'échange d'informations, les analyser et coordonner les opérations entre les Etats membres de l'Union européenne pour lutter contre la criminalité internationale, le terrorisme et l'immigration clandestine. Europol n'est pas à proprement parler une police européenne car il ne dispose pas de pouvoirs coercitifs : ⇨ elle se limite à faciliter l'échange d'informations entre les autorités nationales compétentes ⇨ pour cela, elle gère un système informatisé de recueil d'informations *(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* *et Sylvia Preuss-Laussinotte, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », Cultures & Conflits, n° 74, p. 81-90, été 2009. https://journals.openedition.org/conflits/17441)*
Objectif implicite/ Remarques	Toujours selon Sylvia Preuss-Laussinotte, les nombreux accords de coopération signés par Europol avec des pays tiers et des organisations internationales conduit à un accroissement de la transmission des données personnelles. Cet accroissement des échanges de données pose question quant à la sécurisation des données personnelles. De plus, Europol a accès aux données du SIS et du VIS.
Contenu des données	Nom, prénom, date et lieu de naissance, nationalité, sexe, lieu de résidence, profession, infraction présumée commise par la personne... ↳ *Liste exhaustive des données à l'article 8 du Europol Act 2012* : *http://www.irishstatutebook.ie/eli/2012/act/53/section/8/enacted/en/html#sec8*
Critères d'inscription dans ce fichier	• Une personne a été déclarée coupable d'une infraction pénale • Lorsqu'il existe des motifs raisonnables de croire qu'une personne peut avoir commis une infraction pénale • Lorsqu'il existe des motifs raisonnables de croire qu'une personne est susceptible de commettre une infraction pénale *Europol Act 2012, article 8*
Date de création	26 juillet 1995
Autorité(s) compétente(s)	Europol
Qui a accès à ce fichier ?	• Les Etats-membres (*article 20 du Règlement UE 2016/794 du Parlement européen et du Conseil du 11 mai 2016*) • Les membres du personnel d'Europol dûment habilités par le directeur exécutif (*article 20 du Règlement précité*) • **Eurojust** (Eurojust est l'agence européenne chargée de renforcer la coopération judiciaire entre les Etats membres, pour les poursuites relatives à la criminalité organisée) et OLAF (l'Office européen de lutte antifraude fait partie de la Commission européenne et est chargé d'élaborer la politique de lutte contre la fraude. Il enquête également sur les cas de fraude au détriment du budget de l'UE et sur la corruption et fautes graves commises dans les institutions européennes), dans le cadre de leurs mandats respectifs [peuvent] disposer d'un accès indirect fondé sur un système de concordance/non-concordance (« hit/no hit ») aux informations fournies (…) sans préjudice de toute limitation notifiée par les Etats membres, les organes de l'Union, les pays tiers ou les organisations internationales ayant fourni les informations concernées (*article 21 du Règlement précité*)

Durée de conservation des données	• Les données à caractère personnel traitées par Europol ne sont conservées par celle-ci que pour la durée nécessaire et proportionnée aux finalités pour lesquelles ces données sont traitées. • Europol réexamine, en toute hypothèse, la nécessité de continuer à conserver les données à caractère personnel au plus tard trois ans après le début de leur traitement initial. Europol peut décider de continuer à conserver des données à caractère personnel jusqu'à l'examen suivant, qui a lieu à l'issue d'une nouvelle période de trois ans, si leur conservation reste nécessaire pour lui permettre de remplir ses missions. Les raisons de continuer à conserver les données sont justifiées et consignées. En l'absence de décision de conserver plus longtemps des données à caractère personnel, celles-ci sont effacées automatiquement après trois ans. » *Article 31 du Règlement UE 2016/794 du Parlement européen et du Conseil du 11 mai 2016*
Interconnexion avec d'autres fichiers ?	Europol échange des informations avec des organes et institutions sur la base de traités européens tels que l'Unité de coopération judiciaire de l'Union Européenne (Eurojust), l'Office européen de lutte anti-fraude (OLAF), l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures de l'UE (FRONTEX), le Collège européen de police (CEPOL), la Banque centrale européenne (BCE), l'Observatoire européen des drogues et de la toxicomanie (EMCDDA), Interpol...
Quelle échelle ?	Internationale
Lois qui régissent ce fichier	- 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). *https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32016R0794* - « Europol Act » du 26 décembre 2012. *http://www.irishstatutebook.ie/eli/2012/act/53/enacted/en/pdf* - Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol). *https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32009D0371*
Comment obtenir communication et rectification des données ?	L'accès aux données passe par une demande auprès de l'autorité compétente de l'Etat membre de son choix. L'État membre doit transmettre la requête à Europol dans un délai d'un mois de réception à compter de la réception de la demande. Europol doit par la suite répondre à cette requête dans un délai de trois mois à compter de la réception par Europol de la demande de l'autorité nationale. Europol consulte les autorités compétentes des Etats membres et l'accès aux données se fait en concertation entre Europol et les Etats membres. *Article 36 du Règlement UE 2016/794 du Parlement européen et du conseil du 11 mai 2016*
Sources	- « Europol Act 2012 ». *http://www.irishstatutebook.ie/eli/2012/act/53/enacted/en/pdf* - Sylvia Preuss-Laussinotte, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », Cultures & Conflits, n° 74, p. 81-90, été 2009. *https://journals.openedition.org/conflits/17441* - Site de EUR-Lex, voir ci-dessus les « Lois qui régissent ce fichier ».

Nom du fichier	**INTERPOL**
Sens de l'acronyme	Organisation Internationale de Police Criminelle
Objectif explicite	Interpol est une organisation de coopération policière internationale. Elle fait de la lutte contre la criminalité son objet principal. Lorsqu'on consulte le site internet de l'organisation, différentes activités sont regroupées sous l'onglet « criminalité » : « les atteintes à l'environnement, la corruption, les crimes de guerre, la criminalité financière, la criminalité liée aux véhicules, la criminalité organisée, la criminalité pharmaceutique, la cybercriminalité, le trafic de stupéfiants, la pédocriminalité, le trafic d'êtres humains, le trafic d'armes à feu... ». Liste des 194 Etats membres d'Interpol : *https://www.interpol.int/fr/Pays-membres/Monde* Statut juridique d'Interpol : En 1958, le Conseil économique et social des Nations unies a en effet reconnu à Interpol le statut consultatif d'organisation non gouvernementale. En 1971, l'Organisation a renforcé sa position passant effectivement aux yeux de l'ONU, de la catégorie "organisation non gouvernementale" à la catégorie "organisation intergouvernementale". Buts d'Interpol : *article 2 du Statut d'Interpol* • Assurer et développer l'assistance réciproque la plus large de toutes les autorités de police criminelle, dans le cadre des lois existant dans les différents pays et dans l'esprit de la Déclaration universelle des droits de l'Homme • Etablir et développer toutes les institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun Par conséquent, le mandat de l'Organisation tend non seulement aux développements de la coopération policière internationale mais également au développement des mécanismes de prévention du crime, tant au plan national qu'international. Les données sont traitées dans le Système d'information d'Interpol pour (*article 10 du Règlement d'Interpol sur le traitement des données*) : • retrouver une personne recherchée en vue de la détenir de l'arrêter ou de restreindre ses déplacements • localiser une personne ou un objet présentant un intérêt pour la police • fournir ou obtenir des informations relatives à une enquête pénale ou aux antécédents et activités criminels d'une personne • alerter au sujet d'une personne, d'un évènement, d'un objet ou d'un mode opératoire liés à des activités criminelles • identifier une personne ou un corps • réaliser des analyses de police scientifique • organiser des contrôles de sécurité • identifier des menaces, des tendances en matière de criminalité ainsi que des réseaux criminels
Objectif implicite/ Remarques	Comme le relève l'ACAT (Action des chrétiens pour l'abolition de la torture), le fait qu'Interpol soit « une organisation internationale » fait que « ses agents et les décisions qu'ils prennent bénéficient d'une immunité de juridiction. » Le recours contre une « notice rouge » - message d'alerte international - a « pour seule voie de recours la Commission de contrôle des fichiers d'Interpol ». Cette commission doit veiller « au respect par les organes d'Interpol, des textes régissant l'organisation et notamment des articles 2 et 3 de la Constitution d'Interpol qui doit garantir le respect des droits de l'homme ». Toutefois, les Etats peuvent mettre leur véto à la transmission d'information des personnes fichées par Interpol sur la liste rouge (Site de l'ACAT, « Interpol, au-dessus des lois ? », Hélène Legeay, *https://www.acatfrance.fr/actualite/interpol--au-dessus_des_lois_-*) L'ONG « Fair trial » relève quant à elle que l'usage d'Interpol peut être instrumentalisé à des fins politiques et porter préjudice voire mettre en danger les personnes fichées (Fair Trials International, « Strenghtening respect for human rights, strenghtening Interpol », november 2013, *https://www.fairtrials.org/wp-content/uploads/Strengthening-respect-for-human-rights-strengthening-INTERPOL4.pdf*)

Contenu des données	Plusieurs fichiers : • fichier des noms et alias des individus impliqués et des personnes disparues • fichier des documents de voyages volés et perdus • fichier des véhicules volés • fichier des vols d'œuvres ou objets d'art • fichier d'empreintes et traces digitales • fichier d'empreintes génétiques • fichier d'images d'abus pédosexuels ↳ *Liste complète des fichiers sur le site d'Interpol* : *https://www.interpol.int/fr/Notre-action/Bases-de-donnees/Nos-17-bases-de-donnees* Base de données « nominatives » : Cette base contient des informations relatives aux malfaiteurs internationaux signalés par les pays, en particulier ceux qui sont recherchés. Elle contient également des données sur des personnes disparues et des personnes décédées. L'enregistrement des personnes recherchées dans la base Interpol est réalisé par un message des services d'enquête ou magistrat au BCN Paris sollicitant l'enregistrement de ce malfaiteur dans la base "nominative » d'Interpol. Il peut y être joint tout élément de description y compris photographies, ADN, empreintes digitales ou palmaires... Base de documents de voyages volés ou perdus : Un fichier « SLTD » (stolen and lost travel documents) a été constitué afin de faciliter la détection des documents volés ou perdus. Il recense tous titres de documents de voyage, passeports et autres documents permettant de voyager. L'accès à cette base a été étendu aux services chargés du contrôle des mouvements migratoires (consulats, points frontaliers, aéroports internationaux...). Base SMV (pour « stolen motor vehicles ») sur les véhicules volés : rassemble les identifiants de près de 5 millions de véhicules de tout type. Base des œuvres d'art volées connue comme le fichier « Work of art » : alimentée à partir des images fournies par les services d'enquête des pays participant à ce fichier mais aussi un groupe travail spécifique créé à la suite du vol des biens culturels en Irak. Base des empreintes digitales : empreintes digitales appartenant à des individus identifiés et considérés comme malfaiteurs,traces non identifiées relevées sur les lieux d'infractions. La comparaison ou l'introduction d'une empreinte ou d'une trace est sollicitée par simple message du BCN au Secrétariat général d'Interpol. Base des empreintes génétiques : De la même manière un fichier des empreintes génétiques d'Interpol a été ouvert en 2002. Les empreintes génétiques sont anonymes et seul le rapprochement est possible à l'exclusion d'une identification directe. Base des images d'abus pédosexuels (fichier « ICSE » (Interpol Child Sexual Exploitation database) : banque internationale d'images sur l'exploitation sexuelle des enfants. La base ICSE a pour objet essentiel de permettre aux enquêteurs de confronter les images qu'ils saisissent dans le cadre d'enquêtes, à celles déjà découvertes par les enquêteurs d'autres pays membres d'Interpol.
Critères d'inscription dans ce fichier	→ voir dans « Contenu des données », en fonction des différents fichiers. Par exemple pour le fichier SLTD : lorsqu'une personne qui a déclaré aux autorités nationales son document de voyage perdu ou volé, les détails du document sont transmis à Interpol et entrés dans la base de données SLTD. Les services chargés du contrôle des mouvements migratoires (police aux frontières, compagnies aériennes) peuvent interroger la base de données SLTD afin de déterminer si le document utilisé a été déclaré perdu ou volé.
Date de création	7 septembre 1923
Autorité(s) compétente(s)	Les Bureaux centraux nationaux et le Secrétariat général : • **Les Bureaux centraux nationaux** : chaque Etat membre d'Interpol en désigne un, pour assurer les fonctions de liaison entre l'organisation et les autorités de police de chaque Etat. Ils coordonnent au plan national le traitement dans le Système d'information d'Interpol de données provenant de leur pays. En France, le Bureau Central National (BCN) d'Interpol est situé au sein de la Direction centrale de la Police Judiciaire (DCPJ). La gestion quotidienne du BCN est confiée à la Division des relations internationales (DRI). *https://www.interpol.int/fr/Qui-nous-sommes/Les-pays-membres/Europe/FRANCE* • **Le Secrétariat général** : constitue le centre des échanges de données. Il est chargé de l'administration générale du Système d'information d'Interpol.

	Les Bureaux centraux nationaux émettent des **notices** au Secrétariat national qui les diffuse à chaque pays membre. Ces notices sont « des alertes ou demandes de coopération internationales qui permettent aux services de police des pays membres d'échanger des informations cruciales sur une infraction donnée. » (*https://www.interpol.int/fr/Notre-action/Notices*)
Qui a accès à ce fichier ?	• **Les Bureaux centraux nationaux** → droit d'accès direct au système pour l'exercice de leur fonction statutaires, qui comprend notamment : - l'enregistrement, la mise à jour et l'effacement de données directement dans les bases de données de police de l'Organisation, - la consultation directe des bases de données de police de l'Organisation. ↳ *Liste exhaustive de l'accès des Bureaux nationaux centraux à l'article 6 du Règlement d'Interpol sur le traitement des données* (lien sur le site d'Interpol : *https://www.interpol.int/fr/Qui-nous-sommes/Cadre-juridique/Documents-juridiques*) • **Les entités nationales** → soumises à une autorisation d'accès délivrée par les Bureaux centraux nationaux ↳ *Modalités de délivrance des autorisations à l'article 21 du Règlement d'Interpol sur le traitement des données* (lien sur le site d'Interpol : *https://www.interpol.int/fr/Qui-nous-sommes/Cadre-juridique/Documents-juridiques*) • **Les entités internationales** → par des accords avec l'Organisation ↳ *Modalités pour l'adoption d'un accord à l'article 27 du Règlement d'Interpol sur le traitement des données* (lien sur le site d'Interpol : *https://www.interpol.int/fr/Qui-nous-sommes/Cadre-juridique/Documents-juridiques*) • Concernant la base de données de documents de voyage volés ou perdus (SLTD Database) → l'accès à cette base a été étendu aux services chargés du contrôle des mouvements migratoires (consulats, points frontaliers, aéroports internationaux...)
Durée de conservation des données	« Les données sont enregistrées pour une durée initiale n'excédant pas cinq ans, sous réserve d'une durée de conservation inférieure fixée par le droit national ou de l'accomplissement de ladite finalité. » *Article 49 du Règlement d'Interpol sur le traitement des données*
Interconnexion avec d'autres fichiers ?	Les informations concernant les interconnexions sont difficiles à trouver. Néanmoins, Interpol est interconnecté avec le fichier TES et le fichier API-PNR pour les documents de voyage volés ou perdus. Il partage également des informations avec Europol.
Quelle échelle ?	Internationale
Lois qui régissent ce fichier	- Règlement d'Interpol sur le traitement des données [III/IRPD/GA/2011 (2016)] est la base principale sur laquelle repose l'encadrement légal du traitement des données par cette organisation. Elle repose sur deux grands axes de principes : 1) « Les principes relatifs à la coopération policière internationale » 2) « Les principes relatifs au traitement de l'information » Règlement disponible sur le site d'Interpol, rubrique « Documents juridiques » : *https://www.interpol.int/fr/Qui-nous-sommes/Cadre-juridique/Documents-juridiques* - Statut d'Interpol I/CONS/GA/1956 du 13 juin 1956, disponible sur le site d'Interpol, rubrique « Documents juridiques » : *https://www.interpol.int/fr/Qui-nous-sommes/Cadre-juridique/Documents-juridiques*
Comment obtenir communication et rectification des données ?	« Droits d'accès, de rectification et d'effacement des données : 1. Toute personne ou entité est en droit de saisir directement la **Commission de contrôle des fichiers d'INTERPOL** d'une demande d'accès à des données la concernant traitées dans le Système d'information d'INTERPOL, et/ou de rectification ou d'effacement de telles données. 2. Ces droits d'accès à des données, et/ou de rectification ou d'effacement de données sont garantis par la Commission de contrôle des fichiers d'Interpol et font l'objet d'un règlement distinct. Sauf disposition expresse dudit règlement, les demandes d'accès et/ou de rectification ou d'effacement de données ne peuvent pas être traitées dans le Système d'information d'Interpol. » *Article 18 du Règlement d'Interpol sur le traitement des données*
Sources	- JurisClasseur Droit international, Fasc. 409-10 : « ENTRAIDE JUDICIAIRE INTERNATIONALE. – Organisation internationale de police criminelle – Interpol », 15 Juin 2018. - Site de l'ACAT, « Interpol, au-dessus des lois ? », Hélène Legeay, 4 septembre 2014. *https://www.acatfrance.fr/actualite/interpol--au-dessus_des_lois_-* - Fair Trials International, « Strenghtening respect for human rights, strenghtening Interpol », novembre 2013. *https://www.fairtrials.org/wp-content/uploads/Strengthening-respect-for-human-rights-strengthening-INTERPOL4.pdf* - Site d'Interpol, voir les différentes rubriques citées ci-dessus. *https://www.interpol.int/fr*