anafé

Boîte à fichiers

Un fichier correspond à « *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).

Objectifs de la Boîte à fichiers[1] : L'objectif de la boîte à fichiers est de recenser les traitements de données qui servent aux contrôles des mobilités des personnes étrangères. Dans cette boîte à fichiers, sont recensés :

- Les fichiers par accès direct, c'est-à-dire les fichiers institués directement autour des personnes étrangères, soit dans un but de gestion, soit en tant que fichiers de police,
- Et les fichiers par accès indirect, c'est-à-dire l'enregistrement de données relatives à la condition de personnes étrangères (dites données sensibles) dans des fichiers nationaux et pouvant avoir des conséquences du fait du statut d' « étranger », « étrangère » (par exemple non-obtention du titre de séjour ou de son renouvellement).

Pour chaque traitement de données*, un tableau recense les informations importantes à son sujet ainsi que les liens vers les législations l'encadrant ou d'autres ressources associatives ou académiques relatives audit fichier.

Les fichiers, à l'exception de la base de données relative aux demandes de validation d'attestations d'accueil qui est un fichier municipal, sont classés selon trois échelles géopolitiques : nationale, européenne et internationale. Trois institutions impliquées dans la collecte des données des personnes étrangères sont également détaillées.

Cet outil est à destination des personnes concernées par un fichage, les conseils juridiques (avocats, avocates, militants et militantes associatives…) et toutes les personnes souhaitant participer à mieux comprendre et recenser les outils de surveillance ayant des conséquences pour les personnes étrangères. Pour chaque fichier listé dans le sommaire ci-dessous, il est possible d'obtenir des informations en se référant à un tableau en cliquant sur les acronymes en **gras et souligné**. Les tableaux rassemblent des informations concernant *la date de création, les objectifs, le contenu des données, les critères d'inscription dans le fichier, les autorités compétentes, l'accès au fichier, la durée de conservation, l'interconnexion avec d'autres fichiers, les textes qui régissent le fichier, comment obtenir la communication et la rectification des données.*

La boîte à fichiers 2025 est une actualisation de l'outil créé en 2019, disponible sur Boîte à fichiers 2019 – Anafé. Le nombre de fichiers concernant le contrôle des personnes étrangères a plus que doublé depuis 2019, ce chiffre s'expliquant par l'ajout de fichiers non-pris en compte dans le cadre de la production de la boîte de 2019, l'élargissement des raisons de consultation et d'inscription dans un fichier des personnes étrangères en raison de leur statut d'étranger·ère et enfin la création de nouveaux fichiers, pas encore opérationnels, prévus par le Pacte sur la migration et l'asile (2024) de l'Union européenne (UE). Néanmoins, cet outil n'est pas exhaustif – plusieurs fichiers et institutions n'y figurant pas.

Indication de lecture : Les mots accolés d'une * sont définis dans le glossaire en fin de document.

[1] L'Anafé a choisi d'utiliser un langage « non sexiste » par souci d'égalité entre les genres. Ce document est donc rédigé dans la mesure du possible en utilisant le langage épicène. Par exemple, le choix a été fait d'écrire « personnes en migration » ou « personnes « exilées » plutôt que « migrants ». Cependant pour des commodités de lecture, ce rapport n'utilise pas, hors exception, le « point médian ».

Sommaire

Récapitulatif des fichiers détaillés dans la Boîte à fichiers 3
Fichiers municipaux relatifs aux demandes de validation des attestations d'accueil....6
ACCReD 8
AEM 10
AGDREF 2 13
DNA 17
EASP 19
FAED 22
FIJAIT 25
FNAEG 27
FOVeS 30
FPR 33
France-Visas 37
RMV 2 - Remplacé par France-Visas 39
FSPRT 41
GESI 42
GESTEL 44
GIPASP 45
GIPI 48
INEREC 49
LOGICRA 52
OSCAR 55
PASP 57
SCA ou ADOC 60
SETRADER 63
SILCF 66
TAJ 68
Table de correspondance des noms et prénoms 72
TES 74
VISABIO 78
API-PNR 82
CIR 84
ECRIS-TCN 87
EES 90
ETIAS 94
EURODAC 98
SIS II 104
VIS 109
FIELDS 114
SLTD 115
EUROPOL 117
FRONTEX 120
INTERPOL 123
Glossaire 127
Abréviations 130

Récapitulatif des fichiers détaillés dans la Boîte à fichiers[2]	
Nom	Description
Fichiers municipaux relatifs aux demandes de validation des attestations d'accueil	Ce fichier contient les données des personnes déposant une attestation d'hébergement pour une personne étrangère. Géré par les municipalités, ce traitement de données* a été mis en place en 2005 pour « *lutter contre les détournements de procédure favorisant l'immigration irrégulière* ». (Article R. 142-43 du CESEDA)
ACCReD (Automatisation de la consultation centralisée de renseignements et de données)	Ce fichier a pour finalité la réalisation d'enquêtes administratives. Il est consulté pour l'embauche et le maintien dans des secteurs dits sensibles, les personnes voulant travailler sur un « grand événement », pour une autorisation de port d'arme et pour les personnes demandant un premier titre de séjour, un renouvellement de titre de séjour ou la nationalité française.
AEM (Fichier biométrique d'appui à l'évaluation de la minorité)	Cette base de données contient les données des personnes étrangères se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille. Ces personnes peuvent être orientées par l'aide sociale à l'enfance (ASE) vers la préfecture pour le relevé de leurs empreintes, en vue d'une comparaison avec les fichiers VISABIO et AGDREF 2.
AGDREF 2 (Application de gestion des dossiers des ressortissants étrangers en France)	Ce fichier concerne toutes les personnes étrangères ayant entrepris des démarches relatives au séjour en France. Il permet d'identifier les personnes étrangères présentes sur le territoire et leur statut administratif. Il poursuit un objectif de « *lutte contre la fraude et les fausses identités déclinées sur de faux documents* ».
DNA (Application de gestion du dispositif national d'accueil des demandes d'asile)	Ce fichier contient des données relatives aux demandeurs d'asile en France, dans le but de gérer l'accueil national des personnes demandant l'asile, notamment les orientations vers les lieux d'hébergement et l'octroi des conditions matérielles d'accueil.
EASP (Fichier enquêtes administratives liées à la sécurité publique)	Ce fichier est utilisé pour les enquêtes administratives. Ces enquêtes peuvent intervenir dans le cadre d'une procédure de recrutement ou d'affectation à un poste dans certains secteurs, avec la délivrance d'une autorisation ou d'une habilitation pour accéder à des zones protégées ou à des informations classifiées, en prévision de grands événements et pour les personnes demandant un premier titre de séjour, un renouvellement de titre de séjour ou la nationalité française. Elle concerne toutes les personnes d'au moins 16 ans qui font l'objet d'une enquête administrative.
FAED (Fichier automatisé des empreintes digitales)	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. 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 (Europol et Interpol) ou des services de police étrangers.
FIJAIT (Fichier des auteurs d'infractions terroristes)	Le FIJAIT est utilisé pour « *prévenir le renouvellement des infractions liées au terrorisme* » et « *faciliter l'identification des personnes ayant commis ces infractions* ». Il contient les données des personnes de plus de 13 ans ayant été condamnées, même de manière non définitive ou mises en cause pour des infractions terroristes. Les personnes ayant fait l'objet d'une décision d'irresponsabilité pénale en raison d'un trouble mental à la suite d'une infraction de ce type peuvent également être inscrites dans le FIJAIT.
FNAEG (Fichier national automatisé des empreintes génétiques)	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.
FOVeS (Fichier des objets et des véhicules signalés)	Le FOVeS a pour finalité la découverte et la restitution des véhicules volés, des objets perdus ou volés et la surveillance des véhicules et objets signalés. Il peut également être utilisé à des fins de renseignements, dans le cadre d'enquêtes administratives.
FPR (Fichier des personnes recherchées)	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. La fiche S (atteinte à la sûreté de l'État) fait partie du FPR, elle contient certaines spécificités.
France-Visas	Cette base de données permet d'effectuer des demandes de visa en ligne, de mettre à la disposition des entreprises et institutions habilitées, un espace de dépôt d'invitation en faveur de leurs partenaires étrangers soumis à l'obligation de visa, de traiter les demandes de visas, notamment grâce à l'échange d'informations avec les autorités nationales et les autorités des États mettant en œuvre l'acquis de Schengen. Il est utilisé à des fins de contrôle des migrations et de surveillance des personnes étrangères avant, pendant et après leur séjour en France.
RMV 2 - Remplacé par France-Visas	**Ce fichier n'existe plus, il a été remplacé par France-Visas.** RMV 2 était consulté à chaque instruction de dossier de demande de visa. Y étaient enregistrées toutes les demandes de visas faites dans les consulats français. Cette consultation* permettait de savoir si le demandeur était signalé dans une des autres bases de données auxquelles donnait accès le réseau. En 2023, et après plusieurs opérations de contrôle menées depuis 2020, la Cnil a conclu que le traitement RMV2 fonctionnait de manière illicite et a prononcé un rappel à l'ordre à l'encontre des ministères des affaires étrangères et de l'intérieur.

[2] Dans ce document sont évoqués d'autres fichiers qui n'ont pas été développés en raison de leur éloignement avec la thématique. Ainsi, ne sont détaillés plus bas que les fichiers recensés dans ce tableau.

FSPRT (Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste)	L'objectif officiel de ce fichier est la centralisation des « *informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste, en vue de l'information des autorités compétentes et de leur exploitation par les services et du suivi des personnes concernées* ».
GESI (Gestion des étrangers en situation irrégulière)	Cette base de données comprend les informations des personnes étrangères en situation dite irrégulière interpellées par les services compétents de la préfecture de police et en cours de procédure judiciaire ou administrative. Comme le fichier GIPI, le fichier GESI, remplace le « *fichier des non-admis* », FNAD (abrogé en 2012). Le FNAD était le traitement automatisé de données à caractère personnel des personnes étrangères qui, ayant été contrôlés à l'occasion du franchissement de frontières, ne remplissaient pas les conditions d'entrée requises. Le fichier GESI est aussi un outil opérationnel de police judiciaire à la disposition des agents de ce service, leur permettant d'assurer un suivi en temps réel des procédures judiciaires en cours.
GESTEL (Gestion de l'éloignement)	Créé en 2019, 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. Cette base de données participe à l'identification, au contrôle et à l'éloignement des personnes n'étant pas – au moment du contrôle – régularisées.
GIPASP (Gestion de l'information et prévention des atteintes à la sécurité publique)	GIPASP a pour finalité de « *recueillir, de conserver et d'analyser les informations qui concernent des personnes physiques ou morales ainsi que des groupements dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'État* ». (Article R. 236-21 du code de la sécurité intérieure)
GIPI (Gestion informatisée des procédures d'immigration)	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 personnes étrangères qui ne remplissent pas les conditions d'entrée dans l'espace Schengen entre les États signataires de l'accord de Schengen ainsi que le traitement et le suivi des amendes infligées aux entreprises de transports.
INEREC (Instruction et recours)	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. Le fichier INEREC est consultable via l'interface TélémOfpra. Le personnel de l'Ofpra, les préfectures et le ministère de l'intérieur ont accès à TélémOfpra.
LOGICRA (Logiciel de gestion individualisée des centres de rétention administrative)	LOGICRA a pour finalité la gestion quotidienne et opérationnelle de la rétention administrative des personnes étrangères et de ses différentes étapes et la production de données statistiques. Les données sont conservées deux ans à compter de la sortie définitive du centre de rétention administrative.
OSCAR (Outil de statistique et de contrôle de l'aide au retour)	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.
PASP (Prévention des atteintes à la sécurité publique)	Cette base de données a pour finalité de recueillir, conserver et analyser les informations des personnes d'au moins 13 ans qui concernent les personnes physiques ou morales et les groupements dont l'activité individuelle ou collective qui sont considérés comme pouvant porter atteinte à « *la sécurité publique* » ou à « *la sûreté de* l'État ».
SCA ou ADOC (Système de contrôle automatisé ou accès au dossier des contraventions)	Le fichier SCA/ADOC a été créé en 2004 avec l'utilisation des radars automatiques en France. Ce fichier a été élargi à des fins de contrôles depuis le confinement en avril 2020.
SETRADER (Système européen de traitement des données d'enregistrement et de réservation)	Créé en 2013, ce fichier recense les données des personnes voyageant en avion, à destination ou en provenance d'un « *pays présentant une sensibilité particulière en matière de risque terroriste ou d'immigration irrégulière* » (Délibération n° 2013-016 du 17 janvier 2013). SETRADER a pour finalité la prévention, la répression de l'immigration irrégulière et le contrôle aux frontières ainsi que « *la prévention et la répression des actes de terrorisme et des atteintes aux intérêts fondamentaux* ».
SILCF (Système informatisé concourant au dispositif de lutte contre les fraudes)	Ce traitement est mis en œuvre par la direction générale des douanes et droits indirects afin d'aider à l'exécution des missions de recherche, de constatation, de poursuite et de répression des fraudes.
TAJ (Traitement d'antécédents judiciaires)	Ce fichier contient les données relatives aux personnes interpellées pour des antécédents judiciaires par la police, la gendarmerie nationale et les agents des douanes et judiciaires. Il est utilisé dans le cadre d'enquêtes judiciaires (recherche des auteurs d'infractions), dans le cadre d'enquêtes administratives (par exemple : enquêtes préalables à certains emplois publics ou sensibles) et lors des demandes de titre de séjour et de nationalité française.
Table de correspondance des noms et prénoms	Créé en 2023, ce fichier a pour finalité « *la consultation de l'identité des personnes ayant changé de nom ou de prénom* ». Il enregistre pendant 6 ans les données des personnes ayant réalisées un changement de nom et/ou de prénom administratif.
TES (Titre électronique sécurisé)	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. Depuis 2021, le fichier DOCVERIF[3] reçoit automatiquement les données de tous les passeports et toutes les cartes d'identité (sauf la photographie et les empreintes digitales) du fichier TES. Cela fait de DOCVERIF un fichier-miroir du TES.
VISABIO (Visa biométrique)	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. VISABIO permet en réalité de contrôler de manière stricte les personnes demandant un visa par le biais de l'utilisation des données biométriques* et de limiter l'octroi des titres de séjour pour les personnes étrangères.

[3] Le fichier DOCVERIF est présenté dans la fiche TES mais étant un fichier-miroir du TES, il ne bénéficie pas d'une fiche spécifique. Il convient de se référer à TES et à l'arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF ».

API-PNR (Advance passenger information - personal name record / Renseignements préalables sur les voyageurs - Dossier passager)	Les données de réservation et d'enregistrement des passagers aériens sont contenues dans ce fichier. Ces données sont rapprochées avec d'autres fichiers de polices judiciaire et administrative tel que le FPR, le SIS II ou le SILCF par leur enregistrement dans le système API-PNR.
CIR (Common identity repository / Répertoire commun de données d'identité)	Le traitement CIR vise à stocker les données d'identité, biométriques* et relatives aux documents de voyage renseignées dans les traitements EES, VIS, ETIAS, EURODAC et ECRIS-TCN, afin que celles-ci soient centralisées plutôt que stockées au sein de chacun de ces fichiers. Ainsi, le CIR participe à l'interopérabilité* des systèmes d'information de l'Union européenne (EES, ETIAS, VIS, Eurodac, SIS, ECRIS-TCN). Cette base de données permet une surveillance accrue des personnes étrangères sur le territoire de l'Union européenne (UE).
ECRIS-TCN (European criminal records information system - Third country nationals / Système européen d'informations sur les casier judiciaires – ressortissants de pays tiers)	ECRIS-TCN est « *un système permettant d'identifier les États membres de l'Union européenne (UE) qui détiennent des informations sur les condamnations antérieures de personnes ressortissantes de « pays tiers » et d'apatrides* ». Il contient les informations des ressortissants et ressortissantes de pays hors UE ayant fait l'objet d'une peine privative de liberté (d'au moins six mois) ou d'une infraction pénale punissable d'une peine privative de liberté d'au moins douze mois dans un État membre du l'UE.
EES (Entry-exit system /Système d'entrée-sortie)	Cette base de données contient les données des personnes ressortissantes de « *pays tiers* » à l'UE soumises à un contrôle, non-titulaire d'une carte ou d'un titre de séjour entrant ou sortant du territoire des États membres ou dont l'entrée sur le territoire d'un des États membres a été refusée. L'EES participe à restreindre et contrôler davantage le nombre de personnes étrangères entrant sur le territoire de l'Union européenne.
ETIAS (European Travel Information and Authorisation System / Système européen d'information et d'autorisation concernant les voyages)	L'ETIAS vise à améliorer « *l'efficacité des vérifications aux frontières* », contribuer aux objectifs du système SIS au regard des signalements de personnes non-admises ou faisant l'objet d'une interdiction de séjour, de personnes recherchées, disparues ou des signalements de personnes « *aux fins de contrôles discrets ou de contrôles spécifiques* », contribuer « *à la prévention et à la détection des infractions terroristes ou d'autres infractions pénales graves, et aux enquêtes en la matière* ». L'objectif est de déterminer si la présence d'une personne ressortissante de pays dits tiers sur le territoire d'un État membre *« est susceptible de présenter un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé* » (Article 1 du règlement (UE) 2018/1240) en amont de son arrivée sur le territoire européen.
EURODAC (EU biometric data base / Système de comparaison des empreintes digitales des demandeurs d'asile)	Ce fichier contient les données dactyloscopiques* et en principe les images faciales des demandeurs d'asile et des personnes étrangères entrées irrégulièrement ou en situation dite irrégulière sur le territoire d'un État. Il est utilisé par les États membres pour mettre en œuvre le règlement Dublin sur le traitement des demandeurs d'asile.
SIS II (Schengen Information System II / Système d'information Schengen)	Ce fichier est commun à l'ensemble des États membres de l'espace Schengen et permet à chaque État 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 / Système d'information* sur les visas)	Ce fichier contient les données relatives aux demandes de visas de court séjour. Il permet un échange d'informations entre les États membres pour répondre à divers objectifs notamment lutter contre la fraude ou faciliter l'application du règlement Dublin III.
FIELDS (Frontex-INTERPOL Electronic Library Document System / Système Frontex-INTERPOL d'authentification de documents électroniques)	Le fichier FIELDS est une version de la plateforme Dial-Doc existante d'INTERPOL avec les fiches de vérification rapide de Frontex, pour les mettre à la disposition des agents chargés des contrôles aux frontières via le système mondial de communication policière sécurisée I-24/7 d'INTERPOL. Sur le terrain, le FIELDS est utilisé en première ligne des contrôles aux frontières. Il est utilisé avec les fiches de vérification rapide créées par Frontex. La fiche de vérification rapide est une aide à la décision visuelle. Elle propose un modèle du document qui fait l'objet de la vérification et fait apparaître les principaux éléments de sécurité à vérifier. Les personnes dont les documents sont signalés devront effectuer un contrôle de seconde ligne.
SLTD (Stolen and lost travel documents / Fichier des documents de voyages et d'identité perdus ou volés)	La base de données est accessible via le système mondial de communication policière I-24/7. Elle recense les documents de voyage et d'identité déclarés volés, perdus, révoqués, invalides ou volés vierges. Le fichier SLTD participe à la surveillance accrue et à la limitation de la circulation des personnes étrangères.
EUROPOL (European police office / Agence de l'Union européenne pour la coopération des services répressifs)	Europol est une organisation intergouvernementale destinée à faciliter la coopération policière européenne. Elle permet de faciliter l'échange d'informations entre les États membres, concernant des personnes suspectées ou accusées d'infraction pénale à l'échelle européenne.
FRONTEX (The European Border and Coast Guard Agency / Agence européenne de garde-frontières et de garde-côtes)	Frontex est l'agence européenne de garde-frontières et de garde-côtes. Dans un but opérationnel et statistique, Frontex participe à la collecte et au partage de données des personnes en migration à l'échelle européenne. Frontex « *est à la fois politiquement engagé et légalement obligé de garantir l'utilisation de technologies de pointe pour la surveillance et le contrôle des frontières* ». Elle joue un rôle dans l'influence des priorités de recherche de l'UE en matière de sécurité, notamment en parrainant et/ou commandant des recherches sur les nouvelles technologies pour les contrôles aux frontières.
INTERPOL (International Criminal Police Organization / Organisation internationale de police criminelle)	Interpol est une organisation de coopération policière internationale ayant pour objectif de lutter contre la criminalité. À cette fin, elle met en œuvre un traitement de données* alimenté par des signalements, appelés notices, émis par les pays membres.

Nom du fichier	**Fichiers municipaux relatifs aux demandes de validation des attestations d'accueil**
Sens de l'acronyme	Fichiers des personnes déposant une attestation d'hébergement en municipalité pour une personne étrangère
Date de création	2 août 2005
Quelle échelle ?	Municipale
Objectifs officiels	« *Le maire de la commune du lieu d'hébergement ou, à Paris, Lyon et Marseille, le maire d'arrondissement peut, en qualité d'agent de l'État, mettre en œuvre des traitements automatisés de données à caractère personnel relatifs aux demandes de validation des attestations d'accueil, dont la finalité est de lutter contre les détournements de procédure favorisant l'immigration irrégulière* ». (Article R. 142-43 du CESEDA) Ce fichier est facultatif, les maires n'étant pas tenus d'en créer un.
Objectifs implicites	Comme le dénonce dès 2005, le Gisti, la Ligue des droits de l'homme (LDH) et Imaginons un réseau Internet solidaire : « *La question se pose évidemment de savoir ce que veut dire « lutter contre les détournements de procédure » : en clair, cela signifie qu'une personne ayant accueilli un parent ou un ami étranger qui se maintiendrait ensuite de façon illégale sur le territoire pourrait être suspectée d'avoir organisé ce séjour irrégulier... Il pourrait par la suite être interdit à cette personne (française ou étrangère) de recevoir un autre parent ou ami, et ce non par une décision administrative, ni de justice, mais sur la simple décision d'un maire* ».
Contenu des données	Données relatives à la personne hébergeante : - Identité (nom, prénoms et sexe) et, si la personne agit comme représentante d'une personne morale, sa qualité - Date et lieu de naissance - Nationalité - Type et numéro de document d'identité, ainsi que sa date et son lieu de délivrance si l'attestation d'accueil est signée par une personne de nationalité française - Type et numéro de titre de séjour, ainsi que sa date, son lieu de délivrance et sa durée de validité si l'attestation d'accueil est signée par une personne de nationalité étrangère - Adresse - Données relatives à la situation financière, nécessaires pour apprécier la capacité de prise en charge des frais de séjour et d'hébergement de la personne étrangère - Données relatives aux attestations d'accueil antérieurement signées par la personne hébergeante, s'il y a lieu (nombre, dates, identité de la personne étrangère) Données relatives à la personne hébergée : - Identité (nom, prénoms et sexe) - Date et lieu de naissance - Nationalité - Numéro de passeport - Adresse - Identité et date de naissance du/de la conjointe si la personne est accompagnée par celle-ci - Identité et date de naissance des enfants mineurs, le cas échéant - Données relatives au séjour (durée ainsi que dates d'arrivée et de départ) - Éventuels liens de parenté avec le demandeur - Avis de l'Ofii ou des services de la commune chargés des affaires sociales ou du logement, relatif aux conditions d'hébergement, à la demande du maire - Suites données par l'autorité consulaire à la demande de visa formulée sur la base de l'attestation d'accueil validée Données relatives au logement : - Caractéristiques du logement (surface habitable, nombre de pièces habitables et nombre d'occupants) - Droits de la personne hébergeante sur le logement (propriétaire, locataire ou occupant) (Article R. 142-44 du CESEDA)
Critères d'inscription dans ce fichier	Déposer une demande d'attestation d'accueil pour une personne étrangère auprès de la municipalité de son lieu d'hébergement.

Autorité(s) compétente(s)	Le/la maire de la commune du lieu d'hébergement À Paris, Lyon et Marseille, le/la maire d'arrondissement
Qui a accès à ce fichier ?	Ont accès aux données : - Le/la maire de la commune du lieu d'hébergement ou, à Paris, Lyon et Marseille, le/la maire d'arrondissement, - Les personnels de la mairie individuellement habilités ayant compétence pour instruire les demandes de validation des attestations d'accueil, - Le/la préfet du département et, à Paris, le/la préfet de police, - Les personnels de la préfecture individuellement habilités ayant compétence pour instruire les recours relatifs aux attestations d'accueil. (Article R. 142-45 du CESEDA)
Durée de conservation des données	L'ensemble des données sont conservées 5 ans à compter de la date de validation ou du refus de validation par le maire de l'attestation d'accueil. Les données relatives à l'hébergeant sont effacées lors de son décès ou de son déménagement. (Article R. 142-46 du CESEDA)
Échange de données	« *Les données enregistrées dans les traitements mentionnés à l'article R. 142-43 ne peuvent faire l'objet d'interconnexion, mise en relation ou rapprochement* avec tout autre traitement automatisé de données à caractère personnel* ». (Article R. 142-50 du CESEDA)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas à ce fichier. Les personnes sont, lors du recueil des informations, informées de leurs droits d'accès et de rectification. Selon la Cnil, doit être remis à chaque personne hébergeante une notice d'information portant les mentions prévues par l'article 32 de la loi du 6 janvier 1978 modifiée. Le formulaire « attestation d'accueil » comporte également ces mentions. Le droit d'accès s'exerce auprès de la mairie du lieu d'hébergement ou du/de la maire d'arrondissement pour Paris, Lyon et Marseille. (Article R. 142-48 du CESEDA)
Remarques	La sécurité est garantie, selon la Cnil par l'« *engagement spécifique du maire qu'ont été mises en œuvre des mesures de sécurité et de confidentialité des données et des modalités d'habilitation individuelle des personnels communaux ayant accès au fichier* ». Dans son avis sur le projet de décret (2005), la Cnil avait elle-même estimé qu'une durée de deux ans était suffisante pour détecter un éventuel détournement de procédure. Le gouvernement n'a pas tenu compte des observations de la Cnil. En 2005, le Gisti, la Ligue des droits de l'homme (LDH) et Imaginons un réseau Internet solidaire (IRIS) ont déposé un recours en annulation contre le décret du 2 août 2005 qui autorise les maires à mettre en place des fichiers informatisés permettant le traitement des données collectées à l'occasion de la validation des attestations d'accueil. Leur communiqué dénonce une « *affaire emblématique à la fois des risques que la politique d'immigration fait peser sur les libertés de tous et de l'amoindrissement des garanties que la réforme de la loi « informatique et libertés » d'août 2004 a entraîné en ce qui concerne la protection des données personnelles* ». Comme le rappelle le Gisti et la Quadrature du Net (2022) : « *La mise en œuvre de ce fichier est laissée à l'appréciation du maire, et aucun recensement officiel des communes ayant mis en place un tel outil n'est disponible* ».
Textes qui régissent ce fichier	- Articles R. 142-43 à R. 142-50 du CESEDA - Décret n° 2005-937 du 2 août 2005 pris pour l'application de l'article L. 211-7 du CESEDA et portant sur le traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil - Délibération n° 2005-052 du 30 mars 2005 de la Cnil portant avis sur le projet de décret en Conseil d'État prévu par l'article L. 211-7 du code de l'entrée et du séjour des étrangers et du droit d'asile et relatif aux modalités de mise en œuvre par les maires, agissant en leur qualité d'agents de l'Etat, d'un traitement automatisé de données à caractère personnel relatif aux demandes de validation des attestations d'accueil - 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
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Cnil, Attestations d'accueil des étrangers, consulté en 2025 Gisti, Fichage des hébergeants : Recours contre le décret du 2 août 2005, 2005 Gisti et La Quadrature du Net, Étrangers fichés, 2022

Nom du fichier	**ACCReD**
Sens de l'acronyme	Automatisation de la consultation* centralisée de renseignements et de données
Date de création	3 août 2017
Quelle échelle ?	Nationale
Objectifs officiels	Cette base de donnée a pour finalité de faciliter la réalisation d'enquêtes administratives. (Article 1 du décret n° 2017-1224 du 3 août 2017) D'après le gouvernement, et selon l'article Numerama (2017) : « *la création du fichier ACCReD était indispensable du fait de « l'adoption de nouveaux dispositifs législatifs imposant la réalisation d'enquêtes administratives conditionnant l'accès à certains emplois ou sites sensibles et, d'autre part, par l'évolution des modalités de réalisation des contrôles effectués à l'occasion de ces enquêtes ». Et aussi par le fait qu'il existe depuis de nombreuses années une menace terroriste majeure contre les intérêts français* ».
Objectif implicite	Le fichier ACCReD participe à la généralisation du fichage et étend les possibilités de récolte, d'enregistrement et de traitement des données se rapportant « *à des opinions politiques, philosophiques ou religieuses* ». On peut légitimement s'interroger sur la généralisation du fichage des militants/militantes notamment dans le cadre d'intervention dans les lieux d'enfermement. À travers l'extension des critères d'inscriptions aux personnes demandant un premier titre de séjour, un renouvellement de titre de séjour ou de la nationalité française, il participe à la généralisation du fichage des personnes étrangères du fait de leur statut d'étranger/étrangère ainsi qu'à un rapport de suspicion envers les personnes étrangères. Ce fichier d'enquête administrative participe aux soupçons de délinquance, « *d'atteinte à la sûreté de l'État* » ou de terrorisme spécifiquement envers les personnes étrangères en France.
Contenu des données	Peuvent être enregistrées, dans le traitement les catégories de données à caractère personnel, les informations suivantes : Les données et informations relatives à la demande d'avis, de décisions ou d'éléments d'enquête : - Date de la demande, qualité et coordonnées de la personne à l'origine de la demande, fondement juridique de la demande - Motif de l'enquête : demande initiale, renouvellement et, le cas échéant, éléments circonstanciés Données relatives à la personne faisant l'objet de l'enquête : - Identité (nom de famille, nom d'épouse/époux, prénoms, sexe) - Numéro d'identification fourni par la personne à l'origine de la demande - Date, ville et pays de naissance ; adresse ; nationalité - Emploi, mission ou fonction au titre desquels l'avis, la décision ou les éléments d'enquête sont demandés ; établissement, installation ou zone auquel il est accédé et qualité de la personne au titre de laquelle l'autorisation d'accès est demandée - Immatriculation du véhicule utilisé par la personne au titre de laquelle l'autorisation d'accès est demandée - Type de document d'identité, numéro, date et lieu de délivrance - Niveau d'habilitation (néant, secret, très secret) Données et informations relatives aux résultats de l'enquête : - Indication de l'enregistrement ou non de la personne dans les traitements TAJ, EASP, PASP, GIPASP, FPR, FSPRT, N-SIS II (voir fiche SIS II) et éléments issus de ces traitements, dans la limite des droits définis, pour chacun de ces traitements, au bénéfice des agents mentionnés au I de l'article 5, par l'acte réglementaire qui en autorise la mise en œuvre - Éléments issus des vérifications complémentaires opérées dans le cadre de l'enquête administrative, permettant de déterminer si le comportement de la personne concernée n'est pas soit incompatible avec l'accès à des zones protégées ou avec l'exercice des fonctions ou des missions envisagées ou pour lesquelles elle a été recrutée ou affectée, soit de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'État - Document de synthèse des éléments pertinents issus de l'enquête, contenant les éléments mentionnés aux a à c, accompagné, le cas échéant, du sens de l'avis ou de la décision issues de précédentes enquêtes et relatives à la même personne faisant l'objet de l'enquête - Sens et, le cas échéant, motifs de l'avis ou de la décision ; Date de transmission de l'avis ou de la décision ; Date et sens de la décision de la personne à l'origine de la demande d'avis ; Informations relatives aux recours exercés, le cas échéant, contre l'avis ou la décision (Article 2 du décret n° 2017-1224 du 3 août 2017) Le fichier ACCReD autorise, par dérogation et uniquement dans le cadre des finalités du décret, la collecte, la conservation et le traitement des données se rapportant « à des opinions politiques, philosophiques ou religieuses ». (Article 3 du décret n° 2017-1224 du 3 août 2017)
Critères d'inscription dans ce fichier	Faire l'objet d'une enquête administrative, c'est-à-dire dans le cadre de l'embauche et le maintien à leur poste des personnes travaillant dans les secteurs suivants :

	- Missions de souveraineté de l'État, de sécurité, de défense ; Jeux, paris et courses ; Utilisation de matériels ou produits dangereux ; Emplois en lien direct avec le transport public de personnes, de marchandises dangereuses ; Participation (autrement qu'en simple participant/spectateur) à un grand événement exposé par son ampleur ou par des circonstances particulières à un risque exceptionnel de menace terroriste ; Magistrature et les juges administratifs ; Personnes travaillant dans la police, gendarmerie, les douanes, militaire ou dans le pénitencier ; Personnel de sécurité ; Personnes hauts fonctionnaires ; Les emplois publics et privés exposant leurs titulaires à des risques de corruption ou de menaces liées à la criminalité organisée Il est aussi consulté quand une personne demande une autorisation de port d'arme. Et **pour les personnes demandant un premier titre de séjour, un renouvellement de titre de séjour ou de la nationalité française** (Article L114-1 du code de la sécurité intérieure) (Articles L. 114-1, L. 114-2, L. 211-11-1, R. 114-2, R. 114-3 du code de la sécurité intérieure et article 54 de la loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic (1))
Autorité(s) compétente(s)	La Direction générale de la police nationale et la Direction générale de la gendarmerie nationale (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont accès à ces données, le personnel individuellement désignés et dûment habilités : - du « service national des enquêtes administratives de sécurité » - du service « Commandement spécialisé pour la sécurité nucléaire » Peuvent être destinataires* : - Tout autre personnel d'un service du ministère de l'intérieur, chargé d'effectuer une des enquêtes administratives - Le personnel des services spécialisés de renseignement du ministère de la défense - Les personnes morales ou l'autorité administrative à l'origine de la demande, pour les seules données relatives au sens de l'avis ou de la décision ou, le cas échéant, pour les seules données relatives aux résultats de l'enquête administrative - Le/La préfet de département du lieu d'exercice de l'emploi, de la mission ou de la fonction (dans les conditions mentionnées à l'article 5) (Article 5 du décret n° 2017-1224)
Durée de conservation des données	Les données et informations peuvent être conservées pendant une durée de 5 ans à compter de leur enregistrement.
Échange de données	Interconnexion pour vérifier si l'identité de la personne concernée y est enregistrée avec : le TAJ, EASP, PASP, GIPASP, FPR, FSPRT, N-SIS II (voir fiche SIS II). Les traitements suivants interrogent directement le fichier ACCReD: CRISTINA, GESTEREXT, SIRCID, DGSE (Article 7 du décret n° 2017-1224). En 2023, ont été ajoutés l'extrait B2 du casier judiciaire, deux fichiers d'INTERPOL ainsi que deux fichiers de renseignement non publiés, en l'occurrence selon les informations de la Quadrature du Net, le fichier SIRCID[4] système d'information du renseignement de contre-ingérence de la défense et le fichier TREX[5] de la direction générale de la sécurité extérieure (DGSE). (Décret n° 2023-1388 du 29 décembre 2023)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'information, d'accès, de rectification, d'effacement et à la limitation des données s'exercent directement auprès du ministre de l'intérieur. Les droits mentionnés peuvent faire l'objet de restrictions dans le cadre des enquêtes. La personne concernée par ces restrictions exerce ses droits auprès de la Cnil. Selon la Cnil, si vous êtes concerné par une décision défavorable rendue dans le cadre d'une enquête administrative de sécurité (par exemple, un refus ou une perte d'emploi ou d'habilitation), vous pouvez : - Faire un recours administratif auprès de l'auteur de la décision (recours gracieux) ; - Faire un recours contentieux devant le juge administratif dans les deux mois à compter de la notification de la décision ; - Exercer vos droits d'accès, de rectification ou d'effacement sur vos données personnelles enregistrées dans le fichier dont la consultation* a conduit à la décision défavorable.
Remarques	Comme le rappelle La folle volonté de tout contrôler (2024) : « *En 2020, ACCReD n'a pas été modifié, mais les données contenues dans EASP ont été très largement étendues. Or, les données de ACCReD contiennent automatiquement toutes les données de EASP* ». L'élargissement des interconnexions permet, par voie de conséquences, d'étendre les possibilités de collecte et de transfert d'informations dans le fichier ACCReD.
Textes qui régissent ce fichier	- Articles L. 114-1, L. 114-2, L. 211-11-1, R. 114-2, R. 114-3 du code de la sécurité intérieure - Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation* centralisée de renseignements et de données » (ACCReD)

[4] Le système d'information du renseignement de contre-ingérence de la défense (SIRCID) est un fichier créé en 2022. Le décret n'est pas publié.
[5] Le décret du fichier TREX de la direction générale de la sécurité extérieure n'est pas public.

	- Décret n° 2019-1074 du 21 octobre 2019 modifiant le décret n° 2017-1224 du 3 août 2017 - Décret n° 2022-1243 du 16 septembre 2022 modifiant divers textes pour tenir compte de l'autorisation de mise en œuvre du traitement de données* « SIRCID » - Décret n° 2023-1388 du 29 décembre 2023 modifiant le décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD) et le code de la sécurité intérieure - 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 - Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic (1) - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », Avril 2024 Numerama « 5 questions sur ACCReD, le fichier qui facilite les enquêtes au nom de la sûreté de l'État », 2017 La Quadrature du Net, « Jeux Olympiques : fichage de masse et discrimination politique », 2024

Nom du fichier	**AEM**
Sens de l'acronyme	Fichier biométrique d'appui à l'évaluation de la minorité
Date de création	30 janvier 2019
Quelle échelle ?	Nationale
Objectifs officiels	Le fichier AEM permet selon le gouvernement « *aux conseils départementaux, en charge d'évaluer la minorité et l'isolement des personnes qui se déclarent mineures et qui sollicitent l'aide sociale à l'enfance (ASE) de demander aux services de l'État la vérification de certaines informations de nature à faciliter l'évaluation* ». Le ministre de l'intérieur (direction générale des étrangers en France) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel dénommé « appui à l'évaluation de la minorité » (AEM), ayant pour finalités de mieux garantir la protection de l'enfance et de lutter contre l'entrée et le séjour irréguliers des étrangers en France et, à cet effet : - « *D'identifier, à partir de leurs empreintes digitales, les personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille et ainsi de lutter contre la fraude documentaire et la fraude à l'identité ;* - *De permettre une meilleure coordination des services de l'État et des services compétents en matière d'accueil et d'évaluation de la situation des personnes mentionnées ci-dessus ;* - *D'améliorer la fiabilité de l'évaluation et d'en raccourcir les délais ;* - *D'accélérer la prise en charge des personnes évaluées mineures ;* - *De prévenir le détournement du dispositif de protection de l'enfance par des personnes majeures ou des personnes se présentant successivement dans plusieurs départements.* » (Article R. 221-15-1 du code de l'action sociale et des familles)
Objectif implicite	Ce fichier permet : - D'identifier et empêcher des jeunes de se présenter dans plusieurs départements ; - D'identifier les jeunes reconnu·es majeur·es dans le fichier AGDREF 2 ce qui pourra permettre à la préfecture lors d'un contrôle de mettre en place une procédure d'éloignement du territoire. Le traitement des données dans le fichier AEM peut mener, grâce à l'interconnexion avec le fichier AGDREF 2, au refoulement et/ou au placement en rétention administrative d'une personne étrangère se déclarant mineure, mais ayant été déclarée majeure suite à une procédure d'évaluation de la minorité, sans même que celle-ci n'ait nécessairement eu la possibilité de faire un recours devant un juge des enfants (juridictions des mineurs) contre de cette évaluation. Comme l'avaient soulevé 19 associations en 2019, l'AEM porte atteinte à la protection de l'intérêt supérieur de l'enfant et au droit au respect de la vie privée. (Gisti, Recours déposé contre le décret du 30 janvier 2019 par 19 associations, 2019)

Contenu des données	Les données biométriques* : les images numérisées du visage et des empreintes de deux doigts des personnes qui se déclarent mineures et privées temporairement ou définitivement de la protection de leur famille. Peuvent également être enregistrées dans ce traitement les données à caractère personnel et les informations relatives aux personnes qui se déclarent mineures et privées temporairement ou définitivement de la protection de leur famille suivante : - État civil : nom, prénom(s), date et lieu de naissance, sexe, situation familiale - Nationalité - Commune de rattachement ou adresse de l'organisme d'accueil auprès duquel la personne est domiciliée - Coordonnées téléphoniques et électroniques - Langue(s) parlée(s) - Données relatives à la filiation de la personne (noms, prénoms des parents) - Références des documents d'identité et de voyage détenus et du visa d'entrée délivré - Date et conditions d'entrée en France - Conseil départemental chargé de l'évaluation - Données transmises par le conseil départemental chargé de l'évaluation : a. Numéro de procédure du service de l'aide sociale à l'enfance b. Date à laquelle l'évaluation de la situation de la personne a pris fin et indications des résultats de l'évaluation au regard de la minorité et de l'isolement c. Le cas échéant, existence d'une saisine de l'autorité judiciaire par une personne évaluée majeure et date de la mesure d'assistance éducative lorsqu'une telle mesure est prononcée - Données enregistrées par l'agent de préfecture responsable du traitement : a. Numéro de procédure attribué par le traitement AEM b. Date de la notification au préfet de département et, à Paris, au préfet de police de la date à laquelle l'évaluation de la situation de la personne a pris fin. (Article R. 221-15-2 du code de l'action sociale et des familles) Selon la législation, le traitement ne comporte pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage.
Critères d'inscription dans ce fichier	Personnes se déclarant mineures et privées temporairement ou définitivement de la protection de leur famille.
Autorité(s) compétente(s)	La direction générale des étrangers en France (ministère de l'intérieur)
Qui a accès à ce fichier ?	Peut accéder le personnel individuellement désigné et dûment habilité : - Des préfectures et des sous-préfectures chargé de la mise en œuvre de la réglementation concernant les personnes étrangères ; - Des services centraux du ministère de l'intérieur chargé de l'immigration et du séjour ainsi que des applications et des systèmes d'information relatifs aux étrangers en France. Peut accéder, à des fins exclusives d'établissement de statistiques, aux informations anonymisées obtenues à partir du traitement mentionné à l'article R. 221-15-1 du CASF : - Le personnel chargé des études et des statistiques affectés à la direction générale des étrangers en France et à la direction de la recherche, des études, de l'évaluation et des statistiques du ministère chargé des affaires sociales (voir détails à l'article R. 221-15-1). (Article R. 221-15-3 du CASF) Peuvent être destinataires* des données collectées dans le fichier AEM à l'exclusion de l'image numérisée des empreintes digitales : - Le ou la procureure de la République territorialement compétente et les personnes individuellement désignées et spécialement habilitées par cette dernière ; - Le personnel en charge de la protection de l'enfance du conseil départemental compétent, individuellement désigné et spécialement habilité par le ou la présidente du conseil départemental ; À raison de leurs attributions et dans la limite du besoin d'en connaître. (Article R. 221-15-4 du CASF)
Durée de conservation des données	Les données sont effacées du traitement mentionné à l'article R. 221-15-1 au terme d'un délai maximal d'un an à compter de la notification au préfet de département et, à Paris, au préfet de police de la date à laquelle l'évaluation de la situation de la personne a pris fin. Lorsque le ou la présidente du conseil départemental n'a pas procédé à la notification mentionnée au précédent alinéa, les données sont effacées au terme d'un délai de dix-huit mois à compter de leur enregistrement. (Article R. 221-15-6 du CASF)

Échange de données	En application du décret, la personne se disant mineure peut être orientée dans le cadre de son évaluation vers la préfecture pour le relevé de ses empreintes dans AEM, en vue de sa comparaison avec les fichiers VISABIO et AGDREF 2 et, si la personne est inconnue, de l'enregistrement de ses données personnelles et biométriques* dans le fichier AEM. Ce décret (voir article R. 221-15-5) prévoit par ailleurs la création systématique d'un dossier permettant le transfert de l'ensemble des données personnelles, qui sont toutes des données sensibles, des personnes évaluées majeures, du fichier AEM vers le fichier AGDREF 2.
Comment obtenir communication et rectification des données ?	Selon l'article R. 221-15-9 du CASF, « *le droit d'opposition* prévu à l'article 21 du règlement (UE) 2016/679 [...] ne s'applique pas au présent traitement* ». Le paragraphe II du même article précise que pour obtenir la communication, la rectification et/ou l'effacement des données collectées, la demande doit être déposée auprès du préfet de département et, à Paris, du préfet de police. Ces droits sont encadrés par les articles 15, 16 et 18 du règlement (UE) 2016/679 du 27 avril 2016. En vertu de l'article 18 de ce règlement, le droit à la limitation du traitement des données s'applique si : - L'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ; - Le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ; - Le ou la responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ; - La personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.
Remarques	Le ou la procureure de la République peut accéder à ces données dans un cadre pénal (pour fraude par exemple). Des personnes mineures pourraient donc se retrouver impliquées dans des procédures pénales sans que le processus d'évaluation de leur minorité ne soit achevé, cela ayant des implications sur les garanties applicables en matière de procédure pénale. Dans le cadre de la prise d'empreintes et de données personnelles des enfants, le droit d'opposition* n'est pas garanti par la loi. Cela interroge le respect des protections attachées à la condition de mineur/mineure. En 2019, le Conseil Constitutionnel a rappelé l'importance des règles relatives à la détermination de l'âge d'un individu et aux protections attachées à la qualité de mineur, notamment celles interdisant les mesures d'éloignement et permettant de contester devant un juge l'évaluation réalisée. La majorité d'un individu ne saurait être déduite ni de son refus opposé au recueil de ses empreintes, ni de la seule constatation qu'il est déjà enregistré dans le fichier AEM ou un autre fichier alimenté par les données de celui-ci (Conseil Constitutionnel, 26 juillet 2019, n° 2019-797 QPC). La Défenseure des droits, déplore par ailleurs l'absence de tout bilan d'application dudit fichier par près de 80 départements. Elle relève une incitation de la part des services de l'État par l'article 15 du projet de loi relatif à la protection des enfants, qui en prévoyant le recours obligatoire au fichier AEM « *pourrait porter atteinte au caractère subsidiaire de la consultation* du fichier AEM dans le processus d'évaluation de la minorité et de l'isolement, déjà fortement mis à mal dans la pratique* » (Défenseure des droits, *Les mineurs non accompagnés au regard du droit*, Rapport, 2022). En 2019, 19 associations ont contesté le décret. Plusieurs actions en justice ont été menées, notamment une requête en référé suspension, une requête en annulation et une demande de question prioritaire de constitutionnalité (QPC) qui a été rejetée par le Conseil Constitutionnel. Le Conseil d'État a rejeté la requête le 5 février 2020. (Gisti/Aadjam, La protection des mineures et mineurs isolés étrangers par l'Aide sociale à l'enfance, 2025, pp. 9-11) L'article 40 de la loi n° 2022-140 du 7 février 2022 relative à la protection des enfants oblige tous les départements à transmettre des informations aux préfectures et alimenter AEM sous peine de sanctions financières.
Textes qui régissent ce fichier	- Article R. 221-15 à R.221-15-9 du code de l'action sociale et des familles - Loi n° 2022-140 du 7 février 2022 relative à la protection des enfants - 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 - 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

	- Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Conseil Constitutionnel, 26 juillet 2019, n° 2019-797 QPC Conseil d'État, « Mineurs étrangers non accompagnés : le Conseil d'État valide le décret mais encadre la façon de l'appliquer », 5 février 2020 Défenseure des droits, *Les mineurs non accompagnés au regard du droit*, 2022 Fédération Solidarité, « Fichage des mineurs non accompagnés : un nouveau décret publié », 2019 Gisti, Recours déposé contre le décret du 30 janvier 2019 par 19 associations, 2019 Gisti, Requête en annulation contre le décret du 30 janvier 2019 par 19 associations, 2019 Gisti/Aadjam, La protection des mineures et mineurs isolés étrangers par l'Aide sociale à l'enfance, 2025 InfoMIE, Notes d'observation sur l'AEM, 2020 Pascual Julia, « Le fichier biométrique des « mineurs isolés » déclaré conforme à la Constitution », *Le Monde*, 26 juillet 2019

Nom du fichier	**AGDREF 2**
Sens de l'acronyme	Application de gestion des dossiers des ressortissants étrangers en France Cette application regroupe les fichiers des préfectures et un fichier national (AGDREF 2).
Date de création	8 juin 2011 Le décret du 8 juin 2011 engendre la fusion de l'AGDREF (créé en 1993) et de ELOI (traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement) au sein de l'AGDREF 2.
Quelle échelle ?	Nationale
Objectifs officiels	Selon la Cnil, l'AGDREF 2 a pour finalités de : - « *Garantir le droit au séjour des personnes étrangères en situation régulière ;* - *Lutter contre l'entrée et le séjour irréguliers en France des personnes étrangères*. » À cet effet, il a vocation à : - Permettre aux services du ministère de l'intérieur d'assurer l'instruction des demandes et la fabrication des titres de séjour, de voyage et documents de circulation et la gestion des dossiers des personnes étrangères ; - Mieux coordonner l'action des services chargés de mettre en œuvre des procédures intéressant les personnes étrangères ; - Améliorer les conditions de vérification de l'authenticité des titres de séjour et de l'identité des personnes étrangères 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 personnes étrangères ; - Aider à déterminer et de permettre de vérifier l'identité d'une personne étrangère qui présente une demande d'asile en Guadeloupe, en Guyane, en Martinique, à Mayotte, à La Réunion, à Saint-Martin, à Saint-Barthélemy, à Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie ; - Aider à déterminer et permettre de vérifier l'identité d'une personne étrangère qui se déclare mineure et privée temporairement ou définitivement de la protection de sa famille ; - De permettre aux personnes étrangères de procéder par voie électronique aux formalités prévues par le CESEDA pour la délivrance des titres de séjour ou de document de voyage ou, lorsqu'ils sont titulaires d'un visa de long séjour mentionné aux 6° à 13° et aux 15°, 16° et 17° de l'article R. 431-16 du CESEDA, 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. 142-11 du CESEDA)
Objectifs implicites	Meryem Marzouki, 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 (c'est-à-dire consultable) à la police, à la gendarmerie et aux services de renseignement de la défense à partir de 2007 à la suite d'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 (Meryem Marzouki, 2010). La Cnil a précisé dans la délibération 2018-162 du 17 mai 2018 que le traitement de ce numéro national d'identification unique (numéro AGDREF 2) assigné à chaque personne étrangère figurant dans le traitement éponyme est indispensable pour « *permettre de fiabiliser l'exécution des mesures d'éloignement. En effet, une telle donnée doit permettre de lutter contre les homonymies et les alias et améliorer ainsi l'identification de la personne concernée* ».

	AGDREF contribue à alimenter la logique de suspicion et de fraude à l'encontre des personnes étrangères. Le fait qu'il soit alimenté par d'autres données, relatives notamment à l'éloignement, le transforme en véritable fichier administrativo-policier…
Contenu des données	L'AGDREF 2 contient les images numérisées de la photographie et des empreintes digitales des dix doigts des ressortissants étrangers : - demandeurs et titulaires d'un titre de séjour, d'un titre de voyage supérieur à 1 an ou de la carte de frontalier - en situation irrégulière - faisant l'objet d'une situation d'éloignement - demandeurs d'asile dans les départements, régions et collectivités d'outre-mer D'autres données personnelles : - État civil, Nationalité, Situation familiale, Adresse - Conditions de son entrée en France (entrée régulière ou irrégulière, regroupement familial) - Profession - 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 et contentieux) Données des personnes des proches : - État civil de l'enfant étranger mineur dont les parents font l'objet d'une décision d'éloignement - État civil et filiation de l'enfant français mineur dont les parents sollicitent un titre de séjour en qualité de parent d'enfant français - État civil et adresse du garant - État civil et adresse du responsable du mineur étranger - Adresse complète, nom de l'hébergeant - Ancienne adresse - Pays de résidence antérieure 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 auprès d'un transporteur international...) Liste exhaustive des données à caractère personnel et informations susceptibles d'être enregistrées dans le traitement automatisé AGDREF 2 : annexe 3 du CESEDA Un numéro d'identification national permanent est attribué à chaque personne étrangère figurant dans le traitement.
Critères d'inscription dans ce fichier	Être une personne étrangère : - Qui sollicite la délivrance, auprès d'un consulat ou à la frontière extérieure des États parties à la convention signée à Schengen le 19 juin 1990, d'un visa afin de séjourner en France ou sur le territoire d'un autre État partie à ladite convention ; les empreintes et la photographie sont obligatoirement relevées en cas de délivrance d'un visa ; - Qui, non ressortissante d'un État membre de l'Union européenne, de la République d'Islande, de la Principauté du Liechtenstein, du Royaume de Norvège ou de la Confédération suisse, sollicite la délivrance d'un titre de séjour ; - Qui est en situation irrégulière en France, qui fait l'objet d'une décision d'éloignement du territoire français ou qui, ayant été contrôlée à l'occasion du franchissement de la frontière en provenance d'un pays dit tiers aux États parties à la convention signée à Schengen le 19 juin 1990, ne remplit pas les conditions d'entrée ; - Qui bénéficie de l'aide au retour. (Article L. 142-1 du CESEDA)
Autorité(s) compétente(s)	La direction générale des étrangers en France (ministère de l'intérieur) Les fichiers départementaux sont gérés par les préfectures et le fichier national AGDREF 2 est géré par le ministère de l'intérieur régime mixte RGPD* - Directive « Police-Justice »* auquel est soumis le traitement AGDREF 2 Délibération n° 2020-107 du 29 octobre 2020 de la Cnil

Qui a accès à ce fichier ?	Le personnel individuellement désigné et dûment habilité peut accéder à tout ou partie des données personnelles enregistrées dans le traitement, pour les besoins exclusifs de leurs missions liées à l'entrée, au séjour ou à l'éloignement. Il s'agit du personnel relevant : - du ministère de l'intérieur ; - du ministère de l'Europe et des affaires étrangères ; - des douanes et droits indirects ; - de la police et la gendarmerie nationales ; - des préfectures et des sous-préfectures. Une partie du personnel peut consulter les données pertinentes enregistrées dans ce fichier : - le personnel individuellement désigné et dûment habilité de l'Ofii ; - le personnel individuellement désigné et dûment habilité de l'Ofpra ; - le personnel individuellement désigné et dûment habilité de Pôle emploi ; - le personnel individuellement désigné et dûment habilité des inspecteurs et inspectrices du travail ; - le personnel individuellement désigné et dûment habilité d'organismes de coopération internationale en matière de lutte contre l'immigration irrégulière. (Article R. 142-15 du CESEDA) Peuvent être destinataires* des données, le personnel individuellement désigné et dûment habilité et selon les conditions prévues à l'article R142-16 du CESEDA : - des directions régionales des entreprises, de la concurrence et de la consommation ; - de l'inspection du travail ; - des douanes ; - de l'Office français de protection des réfugiés et apatrides ; - de la direction des libertés publiques et des affaires juridiques ; - de la mission délivrance sécurisée des titres au sein du secrétariat général de ministère de l'intérieur ; - des préfectures et sous-préfectures compétents en matière de prévention et de lutte contre la fraude documentaire ; - des laboratoires du service national de police scientifique, de l'identité judiciaire de la police nationale et de l'institut de recherche criminelle de la gendarmerie nationale ; - du service chargé de la lutte contre la fraude documentaire de la direction nationale de la police aux frontières ; - de la police judiciaire ; - des services fiscaux ; - des organismes chargés de la gestion d'un régime obligatoire de sécurité sociale ; - de l'opérateur France Travail ; - 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 ; - des services spécialisés du renseignement ; - de l'Institut national d'études démographiques ; - de l'Institut national de la statistique et des études économiques et des services statistiques ministériels… (Liste complète à l'article R. 142-16 du CESEDA)
Durée de conservation des données	- Les données relatives aux personnes ayant fait l'objet d'une mesure d'assistance éducative (prononcée par l'autorité judiciaire saisie par la personne intéressée) sont effacées dès la notification de cette mesure d'assistance éducative. - Les données relatives aux personnes ayant acquis la nationalité française sont effacées au terme d'un délai d'1 an à compter du décret de naturalisation ou au terme d'un délai de 6 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 une personne étrangère assignée à résidence sont effacés sans délai après la fin de l'assignation à résidence. - Le dossier qui contient des données relatives à un titre de séjour ou un document de voyage est effacé lorsqu'après l'expiration du document il s'est écoulé un délai de 5 ans sans que le dossier ait fait l'objet d'aucune mise à jour.

	- Le dossier d'une personne étrangère qui contient des données relatives à un arrêté d'expulsion ou à une peine d'interdiction définitive du territoire est **effacé au terme d'un délai de 30 ans après la saisie de la mesure ou de la peine dans le traitement si le dossier n'a fait l'objet d'aucune mise à jour durant les 5 dernières années.** - Le dossier d'une personne étrangère qui contient des données relatives à une peine d'interdiction du territoire à temps prononcée à l'encontre de cet étranger est effacé au terme d'un délai de 5 ans à compter de la caducité de la peine si le dossier n'a fait l'objet d'aucune mise à jour durant cette période. - Le dossier d'une personne étrangère qui contient des données relatives à une interdiction de retour sur le territoire français est effacé au terme d'un délai de 5 ans à compter de l'expiration du délai de validité de l'interdiction, si le dossier n'a fait l'objet d'aucune mise à jour durant cette période. En dehors de ces cas, tout dossier qui n'a fait l'objet d'aucune mise à jour dans un délai de 5 ans à compter de l'enregistrement des premières données qu'il contient est effacé. (Article R. 142-21 du CESEDA)
Échange de données	L'AGDREF 2 est un logiciel* de gestion des fichiers. Il rassemble à la fois des fichiers départementaux (gérés par les préfectures) et un fichier national des dossiers des ressortissants étrangers géré par le ministère de l'intérieur. À l'exception du fichier « IMMI 2 » de l'Ofii, l'ensemble des données contenues dans les fichiers relatifs aux personnes étrangères sont transmises dans le fichier AGDREF 2. Une consultation* simultanée est prévue avec le N-SIS (voir fiche SIS II) et FPR.
Comment obtenir communication et rectification des données ?	Les personnes concernées n'ont pas le droit de s'opposer* au traitement. Les personnes dont les données sont traitées dans AGDREF 2 disposent par ailleurs d'un droit d'accès, d'un droit de rectification et d'un droit à la limitation. Ces droits s'exercent directement : - 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.
Remarques	Lorsque le fichier ELOI a été supprimé, une partie des données relatives à l'éloignement a été intégrée au fichier AGDREF 2. Le décret n° 2019-81 du 6 février 2019 a créé un nouveau fichier spécifique à la gestion des mesures d'éloignement, le GESTEL. La délibération n° 2002-047 du 27 juin 2002 de la Cnil relative à la demande d'avis de la caisse nationale des allocations familiales relative à l'exploitation de certaines données extraites du fichier AGDREF dans le cadre de son obligation de contrôle de la régularité du séjour des personnes étrangères souhaitant bénéficier de prestations familiales a rendu un avis favorable à la transmission de données de l'AGDREF 2 à la CAF. Cela renforce la confusion entre fichier de police et fichier administratif concernant l'AGDREF 2 et les conséquences matérielles du fichage pour les personnes étrangères (ces dernières pouvant perdre un ensemble de ressources et d'aides financières et matérielles à l'émission d'une décision administrative). Dans la délibération n° 2018-162 du 17 mai 2018 de la Cnil relative à la création de ce fichier, cette dernière 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* ». Les données relatives à l'éloignement sont toujours enregistrées dans l'AGDREF 2. Selon la Cnil, « *le traitement AGDREF pourrait évoluer et être remplacé par le système d'information* de l'administration des étrangers en France (« SI AEF »), dans le cadre du programme de développement de l'administration numérique pour les étrangers en France (ANEF)* »[6]. Le Défenseur des droits a publié un rapport sur l'ANEF le 11 décembre 2024. Des bugs sont persistants du fait d'un mauvais paramétrage du basculement entre les bases de données AGDREF et AGDREF 2, la seconde ayant vocation à se substituer à la première selon le Défenseur des droits (2024). Ainsi, des personnes ne peuvent réaliser une nouvelle démarche, et notamment solliciter le renouvellement de leur titre de séjour, au motif – selon le message d'erreur généré par le téléservice ANEF – qu'une demande serait déjà en cours d'instruction.
Textes qui régissent ce fichier	- Article L. 142-1, R. 142-11 à R. 142-25 et Annexe 3 du CESEDA - 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

[6] L'ANEF est une plateforme déployée depuis 2020 qui vise à simplifier les démarches administratives pour les personnes étrangères. Le Défenseur des droits a publié un rapport en 2024 *L'Administration numérique pour les étrangers en France (ANEF) : une dématérialisation à l'origine d'atteintes massives aux droits des usagers* qui dénonce les conséquences de cette dématérialisation sur les droits des personnes étrangères. Il a été décidé de ne pas développer l'ANEF dans cette boîte n'étant pas strictement défini comme étant un « fichier ».

	- Délibération n° 2002-047 du 27 juin 2002 de la Cnil relative au projet de décret présenté par le ministère de l'Intérieur portant modification de l'application de gestion des ressortissants étrangers en France GDREF) et à la demande d'avis de la caisse nationale des allocations familiales relative à l'exploitation de certaines données extraites du fichier AGDREF dans le cadre de son obligation de contrôle de la régularité du séjour des personnes étrangères souhaitant bénéficier de prestations familiales - Délibération n° 2012-293 du 13 septembre 2012 de la Cnil portant avis sur un projet de décret relatif à l'AGDREF et au traitement automatisé de données personnelles relatives aux étrangers - Délibération n° 2013-119 du 16 mai 2013 de la Cnil portant avis sur un projet de décret modifiant le CESEDA - Délibération n° 2018-351 du 27 novembre 2018 de la Cnil portant avis sur un projet de décret modifiant les articles R. 221-11 et R. 221-12 du code de l'action sociale et des familles - Délibération n° 2020-107 du 29 octobre 2020 de la Cnil portant avis sur un projet de décret en Conseil d'État relatif à la mise en place d'un téléservice pour le dépôt des demandes de certains titres de séjour - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Défenseur des Droits, *Rapport - L'Administration numérique pour les étrangers en France (ANEF) : une dématérialisation à l'origine d'atteintes massives aux droits des usagers*, 2024 Cnil, « ADGREF : Application de gestion de dossiers des ressortissants étrangers en France », 2021 Lochak Danièle « Des fichiers pour gérer, contrôler et surveiller les étrangers », *Plein droit*, n° 71, 2006 Marzouki Meryem « Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire ? », *Mouvements*, n° 62, 2010, p. 85-98 Preuss-Laussinotte Sylvia, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, LGDJ, Bibliothèque de droit public, 2000

Nom du fichier	**DNA**
Sens de l'acronyme	Application de gestion du dispositif national d'accueil des demandeurs d'asile
Date de création	20 mai 2009
Quelle échelle ?	Nationale
Objectifs officiels	Ce traitement a pour finalités de permettre à l'Ofii de : - Coordonner la gestion des lieux d'hébergement dédiés aux personnes demandant l'asile et de recenser les offres d'hébergement existantes et disponibles - Procurer les conditions matérielles d'accueil réservées aux personnes demandant l'asile, en évaluant leurs besoins ainsi que leur vulnérabilité - Assurer l'orientation des personnes demandant l'asile et leur répartition dans les centres d'hébergement dédiés, conformément aux schémas national et régionaux d'accueil des personnes demandant l'asile et en fonction des caractéristiques de l'offre et du profil des personnes demandeuses - Vérifier l'acceptation des conditions matérielles d'accueil, et notamment de l'offre d'hébergement, par les personnes demandant l'asile - Allouer l'allocation aux personnes demandant l'asile éligibles, aux personnes titulaires d'un titre de séjour - Assurer l'accompagnement social et administratif - 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 - Informer les personnes demandant l'asile sur les dispositifs d'intégration, de retour et de réinsertion que gère l'office (Article R. 142-51 du CESEDA)
Objectifs implicites	Cela traduit un contrôle accru des personnes demandant l'asile dans une logique générale de suspicion. En effet, comme le souligne Sylvia Preuss-Laussinotte les fichiers de gestion des personnes étrangères – telle que le DNA – s'inscrivent dans une politique générale de lutte contre la fraude où les fichiers sont la clef de voûte des dispositifs mis en place. Ainsi, ces fichiers administratifs et de gestion ont des objectifs de contrôle et se confondent avec les fichiers de police (Sylvia Preuss-Laussinotte, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, 2000).
Contenu des données	- État civil (identité, conditions d'entrée en France, situation familiale, etc.) - Situation administrative au regard du séjour et de la procédure d'asile (Type de procédure, numéros AGDREF (voir fiche AGDREF 2), INEREC (voir fiche INEREC) et éventuellement SKIPPER[7] correspondant au recours formé devant la Cour nationale du droit d'asile du demandeur d'asile, etc.)

[7] Skipper est un logiciel qui est utilisé dans différentes juridictions administratives, il n'est pas centré sur le fichage des personnes étrangères. C'est pourquoi, il n'a pas été développé dans cette boîte.

	- Condition d'accueil (avis du médecin, donnée de détection de la vulnérabilité etc.) - Lieux d'hébergement et d'accompagnement Liste exhaustive à l'annexe 7 mentionnée aux articles R. 142-52, R. 142-53, R. 142-54 et R. 142-56 du CESEDA
Critères d'inscription dans ce fichier	Personne en procédure de demande d'asile en France
Autorité(s) compétente(s)	L'Ofpra, l'Ofii et le Siao (Service intégré d'accueil et d'orientation)
Qui a accès à ce fichier ?	Ont accès à ce fichier : - Les membres du personnel individuellement désignés et spécialement habilités 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 ; - Les agents et agentes chargées de l'accueil des demandeurs d'asile relevant des services centraux et déconcentrés des ministères de l'intérieur et des affaires sociales. Ont un accès limité : les agents et agentes à qui l'Ofii par convention a délégué les prestations d'accueil, d'information et d'accompagnement et les agents et agentes des centres d'accueil pour les personnes demandant l'asile. (Article R. 142-53 du CESEDA) Peuvent être destinataires* des données, les membres du personnel individuellement désignés et spécialement habilités : - de l'Agence de services et de paiement ; - Les personnes appelées à intervenir dans l'instruction des demandes de prise en charge, l'évaluation des personnes demandeuses et leur orientation vers un hébergement, affectées au sein des services intégrés d'accueil et d'orientation du ou des départements concernés ; - Les agents et agentes chargées de l'organisation matérielle des entretiens ainsi que les agents et agentes instructrices chargées de l'audition des personnes demandant l'asile, affectés au sein de l'Ofpra, en cas de détection d'une situation de vulnérabilité pouvant nécessiter des modalités particulières d'examen de la demande par cet organisme, sous réserve du consentement de la personne demandant l'asile ; - Les personnels de santé de l'Ofii pour les données d'état civil du demandeur d'asile et les données relatives à la situation administrative du demandeur d'asile. (Article R. 142-54 du CESEDA)
Durée de conservation des données	Les données et informations enregistrées sont conservées pour une durée maximale de 2 ans à compter de la notification de la décision définitive sur la demande d'asile. (Article R. 142-55 du CESEDA)
Échange de données	Les données du traitement ne font pas l'objet de cession ni d'interconnexion, mise en relation ou rapprochement* avec un autre traitement. Par exception : - Les données d'état civil de la personne demandant l'asile et les données relatives à la situation administrative 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'Ofii est saisi pour émettre un avis dans les conditions fixées par l'article R. 522-2 du CESEDA. - L'Office français de protection des réfugiés et apatrides conserve dans le traitement INEREC les données et informations mentionnées au A du III de l'annexe 7. (Article R. 142-56 du CESEDA)
Comment obtenir communication et rectification des données ?	Il n'y a pas de droit d'opposition. Les droits d'accès et de rectification s'exercent auprès du Directeur général de l'Ofii. (Article R. 142-58 du CESEDA)
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. En 2020, la décision de « *déconcentrer totalement la gestion du DNA au niveau des directions territoriales de l'OFII, en lien avec les services de l'État, en vue de mettre l'ensemble des places à disposition des demandeurs enregistrés localement* » a eu des conséquences sur l'accès à l'application* de gestion DNA. (Schéma national d'accueil des demandeurs d'asile et d'intégration des réfugiés 2021-2023, 2020) Selon, le rapport de Fédération des Acteurs de la Solidarité La gestion des places dans le dispositif national d'accueil (DNA) (2024) : « *si les nouvelles fonctionnalités du système d'information* DNA-NG ayant pour objectif d'encadrer « le volume de places indisponibles et leurs motifs » pourraient avoir pour conséquence de faire baisser les délais d'indisponibilité, en*

	revanche leur fréquence et les ajouts de motifs pourraient augmenter le nombre global de déclarations de places indisponibles dans le DNA et donc produire un taux plus élevé d'indisponibilité ». Pour en savoir plus sur le dispositif national d'accueil des demandeurs d'asile, voir Dispositif d'accueil des demandeurs d'asile : état des lieux 2024 - La Cimade
Textes qui régissent ce fichier	- Articles R. 142-51 à R. 142-8 et Annexe 7 du CESEDA - 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. - Décret n° 2020-1734 du 16 décembre 2020 portant partie réglementaire du CESEDA - Décision n° 2009-202 du 29 mai 2009 relative au traitement automatisé de données relatives aux capacités d'hébergement des centres d'accueil pour demandeurs d'asile, à l'utilisation de ces capacités et aux demandeurs d'asile qui y sont accueillis - Délibération n° 2016-393 du 15 décembre 2016 de la Cnil - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » La Cimade, « Dispositif d'accueil des demandeurs d'asile : état des lieux 2024 », 2024 Fédération des Acteurs de la Solidarité, « La gestion des places dans le dispositif national d'accueil (DNA) », 2024 Preuss-Laussinotte Sylvia, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, LGDJ, Bibliothèque de droit public, 2000 Sadik Gérard, « Fichage des demandeurs d'asile. Le logiciel dn@ corrigé par la Cnil », 2009

Nom du fichier	**EASP**
Sens de l'acronyme	Fichiers enquêtes administratives liées à la sécurité publique
Date de création	16 octobre 2009
Quelle échelle ?	Nationale
Objectifs officiels	Le fichier EASP a pour objectif de : - Faciliter la réalisation d'enquêtes administratives d'orientation et de programmation relatives à la sécurité par la conservation des données issues de précédentes enquêtes relatives à la même personne y compris celles intéressant la sûreté de l'État ; - Identifier les données intéressant la sûreté de l'État. C'est-à-dire celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts. Ces données, de façon isolée ou groupée, font l'objet d'une identification dans le traitement. (Article R. 236-1 du code de la sécurité intérieure)
Objectifs implicites	Il sert notamment à vérifier si une personne peut être admise lorsqu'elle postule à des emplois dans le domaine de la sécurité, de la défense, les jeux, paris, courses, ou qui utilisent des produits dangereux, ou qui induisent l'accès à des zones protégées, par exemple un site nucléaire. Il est également utilisé, depuis la loi n° 2018-778 du 10 septembre 2018, lorsqu'une personne étrangère demande un premier titre de séjour, un renouvellement de titre de séjour ou la nationalité française. Les enquêtes administratives peuvent intervenir : - Dans le cadre d'une procédure de recrutement ou d'affectation à un poste, dans le secteur public ou privé, pour les emplois : qui relèvent de certaines missions de l'État (magistrature, police, etc.) ; dans le secteur de la sécurité ou de la défense (personnel de sécurité, personnels aéroportuaires, etc.) ; au sein d'entreprises de transport public de personnes ou de marchandises dangereuses ; et dans les emplois publics et privés exposant leurs titulaires à des risques de corruption ou de menaces liées à la criminalité organisée ; - Avant la délivrance d'une autorisation, d'un agrément ou d'une habilitation, notamment pour accéder à des zones protégées (sites sensibles) ou à des informations classifiées ; - De telles enquêtes administratives peuvent aussi être menées en prévision de grands évènements sportifs, culturels…
Contenu des données	Peuvent être enregistrées les données suivantes : - Motif de l'enquête

	- Eléments d'identification : nom, prénoms, alias date et lieu de naissance, nationalité, signes physiques particuliers et objectifs, photographies, documents d'identité (type, numéro, validité, autorité et lieu de délivrance), origine géographique (lieux de résidence et zones d'activité) - Coordonnées : numéros de téléphone, adresses postales et électroniques, identifiants utilisés (pseudonymes, sites ou réseaux concernés, autres identifiants techniques) - à l'exclusion des mots de passe, adresses et lieux fréquentés - Situation : situation familiale, formation et compétences, profession et emplois occupés, moyens de déplacement (moyens utilisés, immatriculation des véhicules, permis de conduire), situation au regard de la réglementation de l'entrée et du séjour en France, éléments patrimoniaux - Activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État, activités publiques ou au sein de groupements ou de personnes morales, comportement et habitudes de vie, déplacements, activités sur les réseaux sociaux, pratiques sportives, pratique et comportement religieux - Facteurs de dangerosité : lien avec des groupes extrémistes, éléments ou signes de radicalisation, suivi pour radicalisation, données relatives aux troubles psychologiques ou psychiatriques, obtenues conformément aux dispositions législatives et réglementaires en vigueur, armes et titres afférents, détention d'animaux dangereux, agissements susceptibles de recevoir une qualification pénale, antécédents judiciaires (nature des faits et date), fiches de recherche, suites judiciaires, mesures d'incarcération (lieu, durée et modalités), accès à des zones ou des informations sensibles - Facteurs de fragilité : facteurs familiaux, sociaux et économiques, régime de protection, faits dont la personne a été victime, comportement auto-agressif, addictions, mesures administratives ou judiciaires restrictives de droits, décidées ou proposées - Indication de l'enregistrement ou non de la personne dans les traitements de données à caractère personnel suivants : TAJ, N-SIS (voir fiche SIS II), PASP, GIPASP, FPR, FSPRT, FOVeS (Article R. 236-2 du code de la sécurité intérieure) Est également conservé le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature. Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie. Le traitement ne permet pas d'effectuer des recherches automatisées pour l'ensemble des données – voir les exceptions dans l'article R. 236-2 du code de la sécurité intérieure.
Critères d'inscription dans ce fichier	Personne d'au moins 16 ans faisant l'objet d'une enquête administrative ou demandant un titre de séjour.
Autorité(s) compétente(s)	La Direction centrale de la sécurité publique et par la préfecture de police (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont accès à ce fichier le personnel compétent relevant : - De la direction nationale du renseignement territorial, individuellement désigné et spécialement habilité par la ou le responsable national du renseignement territorial ; - Des services territoriaux de la police nationale chargés du renseignement territorial, individuellement désigné et spécialement habilité par le ou la responsable du service dont il relève ; - Des services de la préfecture de police chargés du renseignement, individuellement désigné et spécialement habilité par le préfet de police. Initialement accessible par la police nationale et les services de renseignement, sa consultation* a été élargie aux douaniers par la loi n° 2023-22 du 24 janvier 2023. Peuvent être destinataires* des données les membres du personnel : - Du service à compétence nationale dénommé « service national des enquêtes administratives de sécurité », individuellement désignés et spécialement habilités par le directeur général de la police nationale ; - Du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire », individuellement désignés et spécialement habilités par la ou le responsable général de la gendarmerie nationale ; - Tout autre personnel d'une unité de la gendarmerie nationale ou d'un service de la police nationale, sur demande expresse précisant l'identité du demandeur ou de la demandeuse, l'objet et les motifs de la consultation. (Article R. 236-6 du code de la sécurité intérieure)
Durée de conservation des données	Les données sont conservées 5 ans. (Article R. 236-4 du code de la sécurité intérieure)
Échanges de données	L'article R. 236-8 du code de la sécurité intérieure qui mentionnait que le traitement ne faisait l'objet d'aucune interconnexion, aucun rapprochement* ni aucune forme de mise en relation avec d'autres traitements ou fichiers a été abrogé en 2017.

	Selon la Cnil : - Lorsqu'ils sont chargés d'une enquête administrative de sécurité, les services compétents peuvent consulter* un certain nombre de fichiers. Il s'agit principalement du : TAJ, N-SIS II (voir fiche SIS II), PASP, GIPASP, FPR, FSPRT, FOVeS ; - Le système ACCReD, créé en 2017, permet de consulter automatiquement et simultanément, via une interconnexion, tous les fichiers précédents. Il est utilisé par le service national des enquêtes administratives de sécurité (SNEAS). L'EASP est donc interconnecté au fichier ACCReD.
Comment obtenir communication et rectification des données ?	Comme le précise la brochure La folle volonté de tout contrôler : « *Jusqu'à la réforme de 2020, la personne était censée être informée que les informations qu'elle donne entrent dans le fichier (Article R. 236-9 du code de la sécurité intérieure issu du décret n° 2013-1113 du 4 décembre 2013). Cette information a été supprimée par le décret n° 2020-1510 du 2 décembre 2020. Le fait de ne pas donner cette information semble avoir été adopté en application de l'article 116 de la loi n° 78-17 du 6 janvier 1978 pour ce qui concerne les données intéressant la sûreté de l'État et de la défense nationale* ». L'article R. 236-9 du code de la sécurité intérieure organise le droit d'accès, de rectification et d'effacement des données contenues dans EASP. Deux types de données sont présentes dans EASP, des données relatives à la prévention et à la détection des infractions pénales, et des données relatives à la sûreté de l'État et à la défense. Par conséquent, deux procédures doivent être menées en même temps pour l'exercice des droits d'accès, de rectification et d'effacement. - Pour l'accès, la rectification et l'effacement des données relatives à la sûreté de l'État et à la défense, il faut s'adresser à la Cnil (Article 118 de la loi du 6 janvier 1978). Le principe de cet article 118 est que lorsque quelqu'un demande à avoir accès à ses données, celles-ci lui sont transmises si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. - Le droit de rectification des données se fait par recours juridictionnel devant la formation spécialisée du Conseil d'État (article R. 841- 2 du code de la sécurité intérieure) créée en 2015 (loi n° 2015-912 du 24 juillet 2015, article L. 773-1 et suivants du code de justice administrative).
Remarques	Le fichier PASP (2009) et le fichier EASP (2009) remplacent EDVIRSP et le projet EDVIGE (voir l'article Jacques Vétois, « Edvige/Edvirsp, Cristina et tous les autres... », 2008). Ce fichier a été modifié par le décret n° 2020-1510 du 2 décembre 2020 afin d'élargir considérablement les données collectées et de supprimer l'obligation d'information. Selon les chiffres de 2020 transmis à l'AFP par le ministère de l'intérieur, début novembre, environ 222 000 personnes étaient inscrites à l'EASP. Comme le précise l'article R. 236-3 : « *L'interdiction prévue au I de l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au fichier EASP (interdiction de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques*, des données biométriques* aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.)* ». Toutefois, « *l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées est autorisé alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale ou qu'il tiendrait à la dangerosité que feraient apparaître les données, obtenues conformément aux dispositions législatives et réglementaires en vigueur, relatives aux troubles psychologiques ou psychiatriques de l'intéressé* ». Comme le précise l'article de Stéphane Pair pour France Info Trois questions sur les fichiers de renseignement que le Conseil d'État a validé au nom de la « sûreté de l'État » (2021) : « *Les syndicats et associations qui ont saisi le Conseil d'État pointent la « dangerosité » et le caractère « flou » des décrets du gouvernement. Ce fichage ne se limitera pas aux individus, aux personnes physiques : il concerne aussi les personnes morales, les associations par exemple. Les opposants à ce système de fichage sont d'autant plus inquiets que ces fichiers du ministère de l'intérieur sont automatisés, c'est-à-dire que les fonctionnaires habilités pourront les renseigner et les interroger en un clic sans intervention d'un juge.* » L'élargissement des fichiers est dénoncé par le Syndicat de la magistrature et le Syndicat des avocats de France. Ils y voient le « spectre du Big Brother en 2021 ». Arthur Messaud, juriste à la Quadrature du Net, estimait en décembre 2020 que le terrorisme était instrumentalisé pour faire « de la surveillance politique » : « *Le gouvernement est largement hors la loi,* [dénonçait-il alors] *[...]Dans ces décrets, il n'est plus seulement question de ficher les personnes considérées comme dangereuses par la police, mais aussi de ficher les personnes qui sont dans l'entourage. Donc, il peut y avoir un bon tiers de la population française* ». De son côté, Yves Veyrier, secrétaire général de Force Ouvrière, dénonçait sur France Info une stigmatisation de l'action syndicale. « *Le fait d'être adhérent d'un syndicat laisserait penser que cela pourrait être associé à des impératifs de sécurité intérieure, de lutte contre le terrorisme, de violences urbaines. Il faut que le gouvernement cesse de jouer avec le feu* ». L'attaque des décrets devant le Conseil d'État est intervenue dans un contexte d'accusations répétées de dérive autoritaire du gouvernement – notamment avec les restrictions imposées dans le cadre de l'état d'urgence sanitaire et la proposition de loi Sécurité globale. Le Conseil d'État a rejeté les recours. Comme le précise Arthur Messaud, porte-parole de La Quadrature du Net au Monde (2020) : « *Nous sommes aussi inquiets : tout ce qui avait été enlevé du fichier Edvige [qui avait fait polémique en 2008], à savoir le fichage des opinions politiques et religieuses, et non plus seulement des activités politiques et religieuses, a été remis », critique-t-il encore. « Comme pour la loi sur le renseignement, on a une pratique jusqu'ici illégale que la police convainc le gouvernement de légaliser a posteriori* ».
Textes qui régissent ce fichier	- Articles R. 236-1 à R. 236-10 du code de la sécurité intérieure

	- Décret n° 2024-616 du 27 juin 2024 relatif à la partie nationale du système d'information Schengen - Décret n° 2023-1013 du 2 novembre 2023 relatif aux services déconcentrés et à l'organisation de la police nationale - Décret n° 2020-1510 du 2 décembre 2020 modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données* à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » - Décret n° 2017-1216 du 2 août 2017 modifiant les traitements automatisés de données à caractère personnel prévus aux articles R. 236-1, R. 236-11 et R. 236-21 du code de la sécurité intérieure - Délibération n° 2020-066 du 25 juin 2020 de la Cnil portant avis sur un projet de décret modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données* à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » (demande d'avis n° 19013317) - Loi n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic (1) - Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Cnil, Les enquêtes administratives de sécurité, 2023 Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 France Inter et AFP, Le Conseil d'État valide l'élargissement des fichiers de renseignement, France Inter, 2021 Guiton Amaelle, L'exécutif lâche la bride aux fichiers de renseignement territorial, Libération, 2020 Pair Stéphane, Trois questions sur les fichiers de renseignement que le Conseil d'État a validés au nom de la «sûreté de l'État«, France Info, 2021 Untersinger Martin, Le gouvernement élargit par décret les possibilités de fichage, Le Monde, 2020 Vétois Jacques, « Edvige/Edvirsp, Cristina et tous les autres... », Terminal, 2008 Vitard Alice, Le recours contre le fichage policier des données personnelles est rejeté par la justice, *Usine digitale*, 2021

Nom du fichier	**FAED**
Sens de l'acronyme	Fichier automatisé des empreintes digitales
Date de création	8 avril 1987
Quelle échelle ?	Nationale
Objectifs officiels	Selon les informations disponibles sur le site du gouvernement, le FAED est un fichier de police qui sert à : - La recherche et l'identification des auteurs de crimes et de délits et à la poursuite, l'instruction, le jugement des affaires criminelles et délictuelles dont l'autorité judiciaire est saisie ; - 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 d'établir les cas de récidive ; - Faciliter la recherche de personnes disparues et l'identification de personnes décédées ou grièvement blessées ; - 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) ; - L'identification et la vérification des titres de séjour d'une personne étrangère dans le cadre de l'article L. 142-2 du CESEDA.
Objectifs implicites	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 (Europol et Interpol) ou des services de police étrangers. Dès sa création en 1987, le FAED a pour objectif implicite le fichage des personnes étrangères. Comme le rappelle Sylvia Preuss-Laussinotte : « *la PAF/DICCILEC s'est toujours efforcée de « multiplier les signalisations d'étrangers interpellés en situation irrégulière et d'alerter le FAED afin d'établir la récidive. Il faut indiquer que la PAF dispose de moyens informatiques permettant d'accéder rapidement aux signalements des étrangers, mais également au FAED.* » (Sylvia Preuss-Laussinotte, Les fichiers et les étrangers au cœur des politiques de sécurité, 2000). La circulaire du 30 avril 1997 indique la finalité claire de l'identification de la personne étrangère en tant que étranger/étrangère non-communautaire notamment pour permettre son éloignement. Selon Jean-Marc Manach (2022), des projets d'interconnexion sont en cours, qui engendreraient un accès grandissant aux empreintes digitales par différents services de l'État.

Contenu des données	En plus des empreintes digitales et palmaires (de la paume de la main), d'autres données sont enregistrées, comme : - La date, le lieu, l'emplacement et les numéros de la collecte et, le cas échéant, l'immatriculation, la marque et le type du véhicule sur lequel l'empreinte digitale ou palmaire a été prélevée - La date et les numéros d'enregistrement dans le fichier - La date des faits, les références aux infractions et au cadre procédural ou juridique de la collecte et les références de la procédure dans le cadre de laquelle l'enregistrement dans le fichier est réalisé - Le sexe, le (s) nom (s), les prénoms, la date, le lieu de naissance, la filiation et la nationalité des personnes dont les empreintes sont collectées dans le traitement - Les clichés anthropométriques* et leur numéro - Pour les seules empreintes mentionnées d'origine inconnue collectées dans le cadre d'une enquête, les nom (s) et prénom (s) de la victime de l'infraction lorsque les nécessités de l'enquête ou de l'information le justifient - Pour les seules empreintes transmises par des organismes de coopération internationale en matière de police judiciaire, des autorités judiciaires ou des services de police étrangers en application d'engagements internationaux : le pays et l'organisme à l'origine de l'information - Les éléments d'identification et le service de l'agent ou l'agente ou du magistrat ayant procédé ou fait procéder aux opérations de collecte, d'enregistrement ou de comparaison - Les informations relatives au contrôle de la qualité des données et celles relatives au procédé technique utilisé pour révéler l'empreinte digitale ou palmaire (Article R. 40-38-3 du code de procédure pénale)
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 concernées par une enquête ou une instruction au cours de laquelle la police recherche les causes d'un décès ou d'une disparition - Les personnes concernées par une enquête ou une instruction qui suit la découverte d'une personne grièvement blessée - Les personnes détenues dans un établissement pénitentiaire - Les personnes victimes ou dont on suppose qu'elles sont victimes d'un enlèvement ou d'une séquestration - Les personnes dont la disparition est inexpliquée
Autorité(s) compétente(s)	La direction centrale de la police nationale (ministère de l'intérieur), sous le contrôle d'un procureur général
Qui a accès à ce fichier ?	Ont accès à ce fichier, les membres du personnel individuellement désignés et spécialement habilités : - De la police nationale et de la gendarmerie nationale affectés dans les services chargés d'une mission de police judiciaire et spécialement chargés de la mise en œuvre du traitement, aux fins de consultation, d'alimentation et d'identification des personnes ; - De la police nationale, de la gendarmerie nationale et les agents et agentes des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires en application des articles 28-1 et 28-2 du code de procédure pénale, aux seules fins de consultation* et d'alimentation ; - Le ou la magistrat chargée du service du casier judiciaire national automatisé et les agents ou agentes de ce service habilitées. (Article R. 40-38-7 du code de procédure pénale) De plus, peuvent consulter les empreintes digitales et palmaires et informations enregistrées dans le fichier, en vue de faire l'objet de comparaisons, les agents et agentes : - D'organismes de coopération internationale en matière de police judiciaire ; - Des services de police ou de justice d'États étrangers ; Aux fins et dans les conditions prévues à l'article R. 40-38-8 du code de procédure pénale. Peuvent être destinataires* des données : - Les officiers et officières et agents et agentes de police judiciaire de la police nationale ou de la gendarmerie nationale ; - Les personnels de la police nationale ou de la gendarmerie nationale ; - Les agents et agentes des douanes et des services fiscaux habilitées à effectuer des enquêtes judiciaires ; - Les personnels de la police nationale et de la gendarmerie nationale chargées de la mise à jour du traitement ; Selon les conditions spécifiées à l'article R. 40-38-7 du code de procédure pénale.

Durée de conservation des données	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 (majeure ou mineure) et du caractère national ou international de la procédure. Elle est au maximum de 25 ans. Pour toutes les durées de conservation, voir l'article R 40-38-4 du code de procédure pénale.
Échange de données	Interconnexion : le traitement Cassiopé[8] (Article R. 15-33-66-4 du code de procédure pénale) En janvier 2024, le gouvernement a déclaré à la Cnil que le FAED fait l'objet d'interconnexions, de rapprochements ou de mises en relation avec les autres traitements suivants : TAJ, FPR, CJN[9], SIS II, EES.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas à ce traitement. Toute demande d'effacement doit, à peine d'irrecevabilité, être adressée par lettre recommandée avec demande d'avis de réception ou formée par déclaration au greffe. Cette demande est directement adressée au procureur de la République compétent, qui est celui de la juridiction dans le ressort de laquelle a été menée la procédure ayant donné lieu à cet enregistrement. Elle peut également être adressée au procureur de la République du domicile de l'intéressé, qui la transmet au procureur de la République compétent. Le magistrat compétent fait connaître sa décision à l'intéressé, par lettre recommandée dans un délai de deux mois à compter de la réception de la demande. A défaut de réponse dans ce délai, ou si le magistrat n'ordonne pas l'effacement, l'intéressé peut exercer un recours devant le président de la chambre de l'instruction dans un délai de dix jours, à compter de l'expiration du délai prévu à l'alinéa précédent ou de la réception par le requérant de la décision du procureur de la République, par lettre recommandée avec demande d'avis de réception ou par déclaration au greffe de la chambre de l'instruction. A peine d'irrecevabilité, ce recours doit être motivé. Le président de la chambre de l'instruction statue, après avoir sollicité les réquisitions écrites du procureur général, par une ordonnance motivée, dans un délai de trois mois à compter de la date de réception de la lettre recommandée ou de la déclaration au greffe par le requérant. Cette ordonnance est notifiée au procureur de la République et, par lettre recommandée à l'intéressé. Elle ne peut faire l'objet d'un pourvoi en cassation que si elle ne satisfait pas, en la forme, aux conditions essentielles de son existence légale. (Article R 40-38-6 du code de procédure pénale) Pour accéder au contenu des données du FAED concernant la personne, il faut écrire au : Service Central de la Police Technique et Scientifique. La demande doit être accompagnée d'une pièce d'identité. En cas de refus ou en l'absence de réponse dans un délai de 2 mois, il est possible de s'adresser à la Cnil via une démarche en ligne. Voir la démarche sur Service Public : fichier automatisé des empreintes digitales (FAED)
Remarques	Le fichier FAED n'a jamais cessé de croître : 1,8 million d'individus fichés en 2004. En décembre 2022, le fichier contenait plus de 6,5 millions d'empreintes de personnes identifiées en tant que mises en cause ainsi que 293 831 empreintes d'origine inconnue. La CEDH a condamné la France en 2013 concernant 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., 18 juillet 2013, *M.K. c/ France*, n° 19522/09). Outre le champ d'application trop extensif du FAED, qui s'étend à des infractions mineures, la Cour a insisté sur les risques de stigmatisation et d'atteinte à la présomption d'innocence des personnes fichées n'ayant pas fait l'objet d'une condamnation par une juridiction de jugement. Pourtant, ce fichier n'a été corrigé qu'à la marge deux ans après l'arrêt de la CEDH, notamment en ce qui concerne les possibilités d'effacement des données et vis-à-vis des durées de conservation (qui reste cependant lié à un jugement décisionnaire de la qualification de la gravité des faits). En septembre 2021, à l'issue de contrôles effectués auprès des services de la police technique et scientifique et de juridictions (tribunaux judiciaires et cours d'appel), la formation restreinte de la Cnil chargée de prononcer les sanctions, avait relevé 5 manquements concernant la manière dont étaient traitées les données du FAED : - La conservation, dans le fichier, de données non prévues par les textes ; - La conservation de données pendant une durée excédant celle prévue par les textes ; - La conservation de données relatives à des personnes ayant bénéficié d'un acquittement, d'une relaxe, d'un non-lieu ou d'un classement sans suite ;

[8] CASSIOPÉE est la Chaîne Applicative Supportant le Système d'Information Orienté Procédure Pénale et Enfants qui est prévue aux articles 48-1 et R. 15-33-66-4 du code de procédure pénale. Les données sont accessibles par les juges, les procureurs/procureures, greffier/greffière, éducateurs/éducatrices de la protection judiciaire de la jeunesse. Il n'a pas semblé central dans le cadre de cette boîte à fichiers qui recense les fichiers de contrôle des personnes étrangères (par accès direct* ou accès indirect*), d'où le fait qu'il n'a pas fait l'objet d'une fiche détaillée.

[9] Le fichier du CJN (casier judiciaire national) enregistre depuis 1984 les condamnations définitives des personnes pour suivi judiciaire et délit. L'Anafé a décidé de ne pas l'inclure dans le cadre de cette boîte à fichiers. Si le CJN peut être demandé pour des démarches administratives relatives à la condition d'étranger/étrangère, il semble que le fichier CJN est peut utiliser directement et que les condamnations sont de manière générale collectées dans la majorité des fichiers relatifs aux contrôles des personnes étrangères déjà mentionnés dans ce document.

	- Une sécurité des données insuffisante en raison d'un mot de passe peu robuste ; - L'absence d'information des personnes concernées.
Textes qui régissent ce fichier	- Articles 78-1 à 78-7 et Articles R. 40-38-1 à R. 40-38-11 du code de procédure pénale - Article L. 235-1 du code de la sécurité intérieure, liant la France à des organismes internationaux ou à des États étrangers - Décret n° 2011-157 du 7 février 2011 modifiant le décret n° 87-249 du 8 avril 1987 (abrogé par le décret n° 2024-374 du 23 avril 2024) relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur - Décret n° 2012-125 du 30 janvier 2012 relatif à la procédure extrajudiciaire d'identification des personnes décédées (procédure extrajudiciaire d'identification des personnes décédées) - 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 - Décret n° 2024-374 du 23 avril 2024 modifiant le code de procédure pénale et relatif au fichier automatisé des empreintes digitales - Délibération n° 2024-006 du 18 janvier 2024 de la Cnil portant avis sur un projet de décret modifiant le code de procédure pénale et relatif à la mise en œuvre d'un traitement de données* à caractère personnel dénommé fichier automatisé des empreintes digitales (FAED) - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Cnil, « Fichier automatisé des empreintes digitales Faed » », 2018 Global Security Mag Online, « FAED : la Cnil clôt l'injonction prononcée à l'encontre du ministère de l'intérieur 01 février 2024 », 2024 Manach Jean-Marc, Le fichier des empreintes digitales sera interconnecté avec le casier judiciaire, Next, 2022 Piazza Pierre, « L'extension des fichiers de sécurité publique », In *Politiques sécuritaires et surveillance numérique*, 2014 Preuss-Laussinotte Sylvia, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, LGDJ, Bibliothèque de droit public, 2000

Nom du fichier	**FIJAIT**
Sens de l'acronyme	Fichier des auteurs d'infractions terroristes
Date de création	24 juillet 2015
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier sert à : - Prévenir le renouvellement des infractions liées au terrorisme ; - Faciliter l'identification des personnes ayant commis ces infractions.
Objectifs implicites	Contrôler et surveiller une partie de la population, sous le contrôle de l'autorité judiciaire. Au vu des usages de la législation « *anti-terroriste* » et des fortes conséquences du fichage au FIJAIT, ce fichier est un outil de contrôle particulièrement attentatoire aux droits. Dans le cadre de la surveillance ambigüe des personnes étrangères, du rapport de suspicion généralisée à leur encontre et de la criminalisation grandissante des personnes migrantes et de leur soutien, le FIJAIT peut être utilisé comme un outil de répression. De plus, une inscription au FIJAIT a des conséquences importantes sur les personnes étrangères, pouvant engendrer le retrait de leur titre de séjour (Conseil d'État, 10e chambre, 18 novembre 2021, n° 444991).
Contenu des données	Informations relatives à l'identité et adresse ou adresses successives du ou des domiciles des personnes fichées. (Article 706-25-4 du code de procédure pénale)
Critères d'inscription dans ce fichier	Être une personne de plus de 13 ans ayant été condamnée, même de manière non définitive ou mise en cause pour des infractions terroristes. Les personnes ayant fait l'objet d'une décision d'irresponsabilité pénale en raison d'un trouble mental à la suite d'une infraction de ce type peuvent également être inscrite dans le FIJAIT. Les actes de terrorisme sont définis comme des infractions commises « *intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur* ». Ces infractions sont listées aux articles 421-1 à 421-6 du code pénal. Elles incluent notamment la provocation et l'apologie du terrorisme.

	En vertu des articles L. 224-1 et L. 225-7 du code de la sécurité intérieure, les personnes n'ayant pas respecté une interdiction de sortie du territoire ou les « règles du contrôle administratif mis en place au retour en France après un déplacement à l'étranger pouvant être lié à des opérations de groupements terroristes » peuvent également faire l'objet d'un enregistrement dans le FIJAIT. Les décisions concernant les personnes mineures âgées de 13 à 18 ans ne sont inscrites dans le FIJAIT que si l'inscription est ordonnée par une juridiction ou le procureur de la République. (Service public et article 706-25-4 du code de procédure pénale)
Autorité(s) compétente(s)	Service du casier judiciaire national (ministère de la justice), et sous contrôle d'un magistrat. (Article 706-25-3 du code de procédure pénale)
Qui a accès à ce fichier ?	Les informations contenues dans le fichier sont directement accessibles, par l'intermédiaire d'un système de communications électroniques sécurisé : - Les autorités judiciaires ; - Les officiers et officières de police judiciaire dans le cadre des procédures concernant les infractions justifiant une inscription dans le fichier ou dans le cadre d'une enquête de flagrance ou d'une enquête préliminaire ou en exécution d'une commission rogatoire ; - Les personnes représentantes de l'État dans le département et les administrations de l'État ; - Le personnel des greffes pénitentiaires habilités et le personnel individuellement désigné ou habilité du bureau du renseignement pénitentiaire de la direction de l'administration pénitentiaire ; - Le personnel individuellement désigné et habilité des services de renseignement ; - Le personnel du ministère de l'Europe et des affaires étrangères habilité. (Article 706-25-9 du code de procédure pénale)
Durée de conservation des données	Les informations relatives à une personne enregistrée dans le FIJAIT sont conservées pour une durée maximale de 20 ans lorsqu'il s'agit d'une personne majeure ou 10 ans lorsque la personne est mineure. Dans les cas des délits suivants - provocation, d'apologie ou d'extraction, de reproduction et de transmission de données faisant l'apologie d'actes de terrorisme ou pour les personnes n'ayant pas respecté une interdiction de sortie du territoire ou une règle de contrôle administratif – les informations sont conservées pour une durée maximale de 5 ans pour une personne majeure et 3 ans pour une personne mineure. Ces délais débutent à partir du prononcé de la décision, ou de la libération de la personne lorsqu'elle a fait l'objet d'une peine privative de liberté. (Article 706-25-6 du code de procédure pénale)
Échanges de données ?	Aucun rapprochement* ni aucune interconnexion ne peut être effectuée entre le FIJAIT et d'autres fichiers, excepté le FPR (et donc le fichier S). (Article 706-25-13 du code de procédure pénale)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits de communication, rectification et effacement des données enregistrées dans le FIJAIT s'exercent auprès du procureur de la République. Lorsque l'inscription a été faite suite à une mise en examen, la demande de rectification ou d'effacement des données peut être faite auprès du juge d'instruction. Si une procédure judiciaire est encore en cours, la demande d'effacement est irrecevable, sauf en cas d'inscription à la suite d'une mise en examen. En cas de refus, le recours peut s'exercer auprès du président de la chambre de l'instruction. (Article 706-25-12 du code de procédure pénale)
Remarques	Les personnes inscrites dans le FIJAIT sont notifiées en personne, par courrier, ou par recours à la force publique par l'officier de police judiciaire (Article 706-25-8 du code de procédure pénale) et doivent se soumettre à certaines obligations administratives, comme le pointage tous les trois mois dans un commissariat ou une gendarmerie ou la déclaration de tout changement d'adresse dans les 15 jours, pour une période de 10 ans à compter du fichage ou d'une sortie de prison lorsqu'il s'agit d'une personne majeure et 5 ans pour une personne mineure. (Article 706-25-7 du code de procédure pénale)
Textes qui régissent ce fichier	- Articles 706-25-3 à 706-25-14 du code de procédure pénale - Articles 421-1 à 421-6 du code pénal - Articles L. 224-1 et L. 225-7 code de la sécurité intérieure
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » David Romain, « Fiché « S », FPR, FSPRT… quels sont les différents fichiers de renseignement utilisés pour la lutte antiterroriste ? », *Public Sénat*, 16 octobre 2023 Service Public, « Fichier des auteurs d'infractions terroristes (FIJAIT) »

Nom du fichier	**FNAEG**
Sens de l'acronyme	Fichier national automatisé des empreintes génétiques
Date de création	Le FNAEG est né de la loi du 17 juin 1998 précisée par le décret du 18 mai 2000
Quelle échelle ?	Nationale
Objectifs officiels	Le FNAEG sert à : - Faciliter l'identification et la recherche des auteurs d'infractions (à l'aide de leur profil génétique) ; - Identifier, dans un cadre judiciaire, une personne décédée dont l'identité est inconnue ou des personnes disparues (à l'aide du profil génétique de leurs proches descendants/ascendants)[10]. (Article R. 53-9 du code de procédure pénale) Les empreintes génétiques sont les séquences d'ADN d'une personne, recueillies à partir de prélèvements effectués à partir des échantillons organiques (sang, sperme, fragments de peau, de cheveux...).
Objectifs implicites	Selon Pierre Piazza : « *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.* » (Pierre Piazza, L'extension des fichiers de sécurité publique, 2009) En 2005, avec le traité de Prüm *relatif à la coopération policière et judiciaire en matière pénale* entre les différents États 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 États membres peuvent ainsi consulter sous certaines conditions les données présentes dans le FNAEG. On constate alors un élargissement progressif des critères d'inscriptions dans ce fichier et du nombre de personnes pouvant voir leurs données génétiques* enregistrées : 65 % des personnes fichées au FNAEG y étaient enregistrées en tant que « personnes condamnées » en 2002, ce pourcentage n'était plus que de 18 % en 2013 sur 2,5 millions de personnes enregistrées. (Réponse du ministère de l'intérieur à une question parlementaire, JO 5 août 2014)
Contenu des données	- Les empreintes génétiques - Les données relatives à la procédure de signalétique, de prélèvement et d'enregistrement - Les données relatives à la nature de l'affaire - Noms, prénoms, date et lieu de naissance et filiation des personnes dont sont recueillis les empreintes génétiques (Article R. 53-11 du code de procédure pénale)
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 d'infractions de nature sexuelle, crime contre l'humanité et les crimes et délits d'atteintes volontaires à la vie de la personne, les crimes et délits de vols, les atteintes aux intérêts fondamentaux de la Nation, les crimes liés au trafic d'armes). Le fichier contient également les empreintes génétiques recueillies à l'occasion de procédures de recherche des causes de la mort ou de recherche des causes d'une disparition, de recherches aux fins d'identification de personnes décédées. (Article 706-54 et Article 706-55 du code de procédure pénale)
Autorité(s) compétente(s)	La direction centrale de la police judiciaire (ministère de l'intérieur), et sous le contrôle d'un magistrat du parquet hors hiérarchie.

[10] La loi prévoit que les échantillons biologiques recueillis sur des cadavres non identifiés peuvent être conservés dans le fichier dans le cadre d'enquête ou d'identification des corps. Cependant aucune précision existe concernant une utilisation généralisée ou systématique pour toutes les personnes mortes aux frontières.

Qui a accès à ce fichier ?	Ont accès à ce fichier : - Le personnel habilité 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 et agentes spécialement habilitées d'organismes de coopération internationale en matière de police judiciaire ou des services de police ou de justice d'États étrangers - Les magistrats et magistrates du parquet et de l'instruction, les officiers et officières de police judiciaire, les personnes physiques ou morales agréées ayant réalisé les analyses, et les personnels agissant sous leur responsabilité Les officiers et officières, les agents et agentes de police judiciaire ainsi que les personnels spécialisés, techniciens ou ingénieurs de police technique et scientifique qui ne peuvent pas accéder à l'ensemble des données (Article R. 53-18 du code de procédure pénale)
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 - 40 ans : pour les données récolté dans le cadre d'enquête de crimes contre l'humanité, atteintes volontaires à la vie, tortures et actes de barbarie, crimes et délits de violences volontaires, viols, agressions sexuelles, trafic de stupéfiants, enlèvement et séquestration, détournement de tout moyen de transport, traite des êtres humains, proxénétisme, recours à la prostitution de mineurs ou de personnes vulnérables, mise en péril de mineurs, vol avec violences, crime de vols, crimes d'extorsion, destructions, dégradation et détériorations dangereuses pour les personnes, trahison et espionnage, attentat et complot, mouvement insurrectionnel, usurpation de commandement, levée de forces armées et provocation à s'armer illégalement, actes de terrorisme, fausse monnaie, participation à une association de malfaiteurs, infractions au régime des armes et munitions - 25 ans : pour les données des personnes mises en cause pour des infractions autres que celles mentionnées ci-dessus - 25 ans : pour les empreintes génétiques des personnes ascendantes ou descendantes d'une personne disparue prélevées avec leur accord (disparition inquiétante ou suspecte) (Voir les informations complémentaires à l'article R. 53-14 du code de procédure pénale)
Échange de données	Le FNAEG est interconnecté avec : CASSIOPÉE, LRPPN[11] et LRPGN[12], la passerelle internationale en matière d'ADN d'INTERPOL (Décret n° 2021-1402 du 29 octobre 2021 modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques et Article R 53-19 du code de procédure pénale). Avec la décision 2008/615/JAI du Conseil de l'UE relative à la coopération transfrontalière, les fichiers nationaux d'empreintes génétique de l'UE peuvent faire l'objet de rapprochements - 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.

[11] LRPPN (Logiciel de Rédaction des Procédures de la Police Nationale) alimente automatiquement le TAJ, FOVeS et CASSIOPEE et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer dans le présent document au vu de sa proximité avec le TAJ et le FAED. Pour les informations complémentaires, voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

[12] LRPGN (Logiciel de Rédaction des Procédures de la Gendarmerie Nationale) alimente automatiquement le TAJ, FOVeS et CASSIOPEE, et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer dans le présent document au vu de sa proximité avec le TAJ et le FAED. Pour les informations complémentaires, voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'information et d'accès s'exercent auprès du chef du service national de police scientifique du ministère de l'intérieur. La demande d'effacement des données se fait auprès du procureur de la République de la juridiction dans le ressort de laquelle la procédure a été menée et a donné lieu à l'enregistrement. La demande d'effacement est d'autant plus importante que la personne n'aura pas été condamnée pour les faits en question. En cas de refus d'effacement, il faut faire un recours devant le JLD. Et en cas de nouveau refus du JLD, il faut faire un recours devant le Président de la chambre de l'instruction. Le formulaire CERFA de demande d'effacement des données du FNAEG est en ligne sur le site du ministère de la Justice. Pour les mineurs, la demande doit être faite par le représentant légal.
Remarques	Comme le décrit Virginie Gautron dans le Répertoire de droit pénal et de procédure pénale : « *Dès le début de la décennie 1990, de multiples textes internationaux, de portée contraignante ou incitative ont invité les États à développer les analyses de l'acide désoxyribonucléique (ADN) dans le cadre du système de justice pénale. Plusieurs pays ont constitué de tels fichiers bien avant la France, comme la Grande-Bretagne, l'Écosse, les Pays-Bas, l'Autriche, l'Allemagne, la Finlande et la Norvège. La France a introduit les méthodes d'analyse et d'identification par empreintes génétiques en 1994, à l'occasion des lois dites de bioéthique, l'article 16-11 du code civil posant seulement le principe de la licéité de ces méthodes.* ***Ce fichier a commencé à fonctionner en juin 2001, avant que plusieurs lois ne viennent étendre son champ d'application***. » En 2008, la Cour européenne des droits de l'Homme a condamné la Grande-Bretagne dans une affaire relative à son fichier d'empreintes génétiques (CEDH, 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n° 30562/04 et 30566/04), notamment en raison du « *caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions, mais non condamnées* ». Si des reproches similaires pouvaient être adressées au FNAEG, des requêtes de ressortissants français ont été déclarées irrecevables par la Cour, mais pour avoir sciemment divulgué le détail des propositions de négociation amiable formulées par le gouvernement français (CEDH, Sect. 5, 13 décembre 2011, *Mandil c/ France*, n° 67037/09 ; CEDH, Sect. 5, 13 décembre 2011, *Barreau et a. c/ France*, n° 24697/09). En 2011, selon le rapport de Delphine Batho et Jacques Alain Bénisti relatif aux fichiers de police, l'interconnexion des fichiers d'identification et d'antécédents (FAED, FNAEG et TAJ) était à l'étude, avec pour objectif de « *fiabiliser les données intégrées dans le fichier TAJ et de repérer plus aisément l'utilisation d'alias ou les problèmes d'homonymie* ». Selon l'article 706-56 du code de procédure pénale, l'officier ou l'officière de police judiciaire peut procéder, ou faire procéder sous son contrôle, au prélèvement biologique destiné à permettre l'analyse d'identification de leur empreinte génétique. Les personnes requises conformément à l'alinéa précédent peuvent procéder, par tous moyens y compris télématiques, à la demande de l'officier ou l'officière de police judiciaire, du/de la procureur de la République ou du/de la juge d'instruction, aux opérations permettant l'enregistrement des empreintes dans le fichier national automatisé des empreintes génétiques. Les officiers et officières de police judiciaire peuvent également, d'office ou à la demande du/de la procureur de la République ou du/de la juge d'instruction, faire procéder à un rapprochement* de l'empreinte de toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis l'une des infractions mentionnées à l'article 706-55 avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée. Le fait de refuser de se soumettre au prélèvement biologique est puni d'un 1 d'emprisonnement et de 15 000 euros d'amende. Lorsqu'une personne a été condamnée pour crime, le refus de se soumettre au prélèvement biologique est puni de 2 ans d'emprisonnement et de 30 000 euros d'amende. Selon la Cour de cassation, la condamnation du prévenu pour refus de se soumettre au prélèvement biologique ne porte pas atteinte au droit au respect de sa vie privée dans la mesure où il existe une possibilité concrète, en cas d'enregistrement de son empreinte génétique au fichier, d'en demander l'effacement. (Cour de cassation, 15 janvier 2019, n° 17-87.185) Nombreux sont ceux qui déplorent en France le détournement de la loi de son but premier, notamment pour poursuivre des représentants syndicaux qui refusent que soit effectué sur eux un prélèvement génétique (voir le rapport de Delphine Batho et Jacques Alain Bénisti relatif aux fichiers de police). Une jurisprudence de la CEDH datant de 2017 (CEDH, 5e Sect., 22 juin 2017, *Aycaguer c/France*, n° 8806/12) a condamné la France, estimant que le FNAEG portait une « atteinte disproportionnée » à la vie privée. Le juge européen avait en effet été saisi par un agriculteur qui avait refusé un prélèvement d'ADN après avoir été condamné à deux mois de prison avec sursis pour avoir donné un coup de parapluie en direction de CRS, lors d'une manifestation organisée par un syndicat et qui avait été émaillée de quelques accrochages avec les forces de l'ordre. La Cour européenne avait relevé « *qu'aucune différenciation n'est actuellement prévue en fonction de la nature et de la gravité de l'infraction commise, malgré l'importante disparité des situations susceptibles de se présenter* ». (Grégoire Lecomte Rulez, Fichier des empreintes génétiques : la France condamnée par la CEDH pour défaut d'encadrement, 2021)

Textes qui régissent ce fichier	- Articles 706-54 à 706-56-1 et Articles R. 53-9 à R. 53-21 du code de procédure pénale - Décret n° 2012-125 du 30 janvier 2012 relatif à la procédure extrajudiciaire d'identification des personnes décédées - Décret n° 2021-1402 du 29 octobre 2021 modifiant le code de procédure pénale et relatif au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques - Arrêté du 22 novembre 2023 relatif au conditionnement normalisé et au traitement subséquent des scellés adressés au service central de préservation des prélèvements biologiques - 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 - Délibération n° 2008-113 du 14 mai 2008 de la Cnil portant avis sur un projet de décret en Conseil d'État modifiant le code de procédure pénale et relatif au fichier national des empreintes génétiques - Délibération n° 02-008 du 7 mars 2002 de la Cnil relative à l'extension des conditions pour être inscrit dans ce fichier - Directive (UE) 2016/680 « Police-Justice »* : traitement des données personnelles en matière d'infractions pénales - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Batho Delphine et Bénisti Jacques Alain, N°4113 - Rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, 2011 Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 Cnil, « FNAEG : Fichier national des empreintes génétiques », 2018 Lecomte Rulez Grégoire, « Fichier des empreintes génétiques : la France condamnée par la CEDH pour défaut d'encadrement », Next, 2017 Manach Jean-Marc, « Plus d'un tiers des Français sont fichés dans le FNAEG », Next, 27 septembre 2021 Piazza Pierre, « L'extension des fichiers de sécurité publique », *Revue Hermes*, n° 53, 2009

Nom du fichier	**FOVeS**
Sens de l'acronyme	Fichier des objets et des véhicules signalés
Date de création	7 juillet 2017, en expérimentation dès 2014
Quelle échelle ?	Nationale
Objectifs officiels	Ayant pour finalités de faciliter les recherches et les contrôles de la police, de la gendarmerie et des douanes dans le cadre de leurs attributions respectives pour : - La découverte et la restitution des véhicules volés ; - La découverte et la restitution des objets perdus ou volés ; - La surveillance des véhicules et objets signalés. Ce traitement peut faire l'objet d'une consultation, lors de la réalisation des enquêtes administratives prévues aux articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure. (Article 1 de l'arrêté du 7 juillet 2017 portant sur l'autorisation d'un traitement automatisé de données à caractère personnel dénommé Fichier des objets et des véhicules signalés)
Objectif implicite	Retrouver les objets et les véhicules volés, et surveiller les objets et les véhicules signalés. Il peut également être utilisé à des fins de renseignement. En effet, en cas d'enquête administrative sur une personne qui souhaite travailler dans des métiers dit sensibles (au sens des articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure), gendarme, policier ou militaire.
Contenu des données	Données concernant les vols et découvertes : - Vols : nature de l'objet (ou de l'animal) ou du véhicule ; numéro de série et autre numéro d'identification ; photographies de l'objet ou du véhicule ; date de la photographie ; numéro de procédure ; date et heure de plainte ; date, heure et lieu du vol ; coordonnées du service de plainte ; état civil et coordonnées du propriétaire, du plaignant ou du titulaire pour les documents ; le cas échéant, identité de la personne susceptible d'utiliser le véhicule ou l'objet ; code de la compagnie d'assurance et numéro de police du véhicule ; descriptifs et caractéristiques complémentaires de l'objet ; conduite à tenir en cas de découverte

	- Découvertes : Outre les données précitées relatives aux vols, sont également enregistrées les informations suivantes : numéro de procédure de découverte ; date, heure et lieu de découverte ; coordonnées du service de découverte ; descriptif complémentaire de l'objet Données concernant les surveillances et cessations de surveillances : - Surveillances : nature de l'objet ou du véhicule ; numéro de série et autre numéro d'identification ; numéro de procédure ou numéro d'ordre administratif ; cadre juridique ; date de mise sous surveillance ; coordonnées du service demandeur et, lorsqu'il diffère, du service inscripteur ; photographies de l'objet ou du véhicule [date de la photographie] ; le cas échéant, identité de la personne susceptible d'utiliser le véhicule ou l'objet ; conduite à tenir ; descriptif et caractéristiques complémentaires de l'objet ; date et heure de cessation de la surveillance - Cessations de surveillances : Outre les données précitées relatives aux surveillances, sont également enregistrées les informations suivantes : numéro de procédure ou numéro d'ordre administratif de cessation ; motif, date et heure de cessation de surveillance Données concernant les pertes et découvertes : - Pertes : nature de l'objet ; numéro de série et autre numéro d'identification ; numéro d'ordre administratif ; date et heure de déclaration de perte ; date, heure et lieu de la perte coordonnées du service saisi ; propriétaire : état civil et coordonnées ; descriptif et caractéristiques complémentaires de l'objet ; conduite à tenir - Découvertes : outre les données précitées relatives aux pertes, sont également enregistrées les informations suivantes : numéro d'ordre administratif de découverte ; date, heure et lieu de découverte ; coordonnées du service de découverte (Annexe de l'arrêté du 7 juillet 2017)
Critères d'inscription dans ce fichier	Le traitement est constitué des données à caractère personnel et informations issues : - Des procédures judiciaires diligentées pour des faits de vol établies par les services de la police nationale ou par les unités de la gendarmerie nationale ; - Des mesures de surveillance exécutées par les services de la police nationale, les unités de la gendarmerie nationale ou les services des douanes ; - Des déclarations de perte effectuées auprès des services habilités à les recevoir ; - Des décisions d'invalidation de documents prononcées par les autorités administratives ; - Des traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers, dans les conditions énoncées à l'article L. 235-1 du code de la sécurité intérieure. (Article 2 de l'arrêté du 7 juillet 2017) - L'inscription dans le fichier FOVes est effectuée par les services de police ou les unités de la gendarmerie nationales. - L'inscription d'une mesure de surveillance peut également être effectuée par les services des douanes. - L'inscription d'un document invalidé par décision d'une autorité administrative peut être effectuée par la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur. - Pour les véhicules ou objets déclarés volés, cette inscription est effectuée dans les meilleurs délais après le dépôt de plainte. (Article 3 de l'arrêté du 7 juillet 2017)
Autorité(s) compétente(s)	La direction générale de la police nationale et direction générale de la gendarmerie nationale (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont accès à tout ou partie des données à caractère personnel et informations mentionnées à l'article 2, à raison de leurs attributions légales et dans la limite du besoin d'en connaître : - Le personnel des services de la police nationale, individuellement désigné et habilité ; - Les militaires des unités de la gendarmerie nationale, individuellement désignés et habilités ; - Le personnel douanier, individuellement désigné et habilité ; - Le personnel de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur, individuellement désigné et habilité ; - Le personnel du service à compétence nationale dénommé « Unité Information Passagers » rattaché au ministère chargé du budget, individuellement désigné et habilité ; - Le personnel du service à compétence nationale dénommé « Service national des enquêtes administratives de sécurité » rattaché à la direction générale de la police nationale, individuellement désigné et habilité par le directeur général de la police nationale ; - Le personnel du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire » relevant du ministre chargé de l'énergie et du ministre de l'intérieur et rattaché à la direction générale de la gendarmerie nationale, individuellement désigné et habilité par le directeur général de la gendarmerie nationale. Peuvent être destinataires*, dans le cadre de leurs attributions légales et dans la limite du besoin d'en connaître, de tout ou partie des mêmes données et informations : - Les autorités administratives en charge de l'immatriculation des véhicules, de la gestion des titres sécurisés et de la délivrance d'autorisations de détention et d'acquisition d'armes ;

	- Les organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers dans les conditions énoncées à l'article L. 235-1 du code de la sécurité intérieure ; - Les agents et agentes de la police municipale ; - Le personnel de contrôle de la préfecture de police exerçant leurs fonctions dans la spécialité voie publique et le personnel de surveillance de Paris ; - Les organismes d'assurance liés par un protocole d'accord avec le ministère de l'intérieur pour les seules informations relatives aux véhicules volés et découverts ; - Les autorités judiciaires ; - Le service statistique ministériel de la sécurité intérieure. (Article 4 de l'arrêté du 7 juillet 2017)
Durée de conservation des données	- Pour les véhicules et objets volés sont conservées pendant 5 ans pour les moyens de paiement et les appareils audiovisuels ou objets divers ; 10 ans pour les véhicules (véhicules terrestres, bateaux et aéronefs), documents, conteneurs et équipements industriels, plaques d'immatriculation, certificats d'immatriculation et moteurs de bateau ; 20 ans pour les billets de banque ; 50 ans pour les armes, munitions, explosifs, bijoux, montres, horlogeries et objets d'art. - Pour les objets perdus sont conservés pendant 10 ans pour les documents ; 50 ans pour les armes. - Pour les véhicules et objets surveillés sont conservées pendant une durée maximale de 6 mois renouvelables. - En cas de découverte ou de fin de surveillance avant les délais fixés précédemment, les données sont conservées pendant 4 mois. Cette durée est portée à 5 ans pour les seules découvertes de véhicules terrestres, de bateaux et de moteurs de bateau. Elles sont uniquement accessibles aux administrateurs du traitement. - À l'issue de ces délais, les données sont supprimées du traitement et archivées pendant une durée de 10 ans. Elles sont uniquement accessibles au seul exploitant technique du traitement, sur demande expresse et écrite des administrateurs du traitement. (Article 5 de l'arrêté du 7 juillet 2017) Les opérations de création, consultation, modification et suppression font l'objet d'un enregistrement comprenant l'identification de l'auteur, la date, l'heure et la nature de l'opération. Ces informations sont conservées pendant 5 ans. (Article 7 de l'arrêté du 7 juillet 2017)
Échanges de données	Interconnexion avec SIS II. Interconnexion pour vérifier si l'identité de la personne concernée y est enregistrée avec Interpol, LAPI, PASP, GIPASP, EDVIGE, API-PNR, Fichier National des Interdits de Stade (FNIS)
Comment obtenir communication et rectification des données ?	Les droits d'information et d'opposition ne s'appliquent pas. Par exception, les victimes de vol et les propriétaires d'objets perdus sont informés qu'ils peuvent faire l'objet d'une inscription dans ce traitement. - Pour les données relatives aux véhicules et aux objets surveillés : le droit d'accès s'exerce de manière indirecte auprès de la Cnil. - Pour les données relatives aux véhicules volés, aux objets volés ou perdus et aux documents invalidés : le droit d'accès s'exerce directement auprès de la DGPN ou de la DGGN, sous certaines conditions prévues au dernier alinéa de l'article 41 de la loi n° 78-17 du 6 janvier 1978. (Article 8 de l'arrêté du 7 juillet 2017)
Remarques	Les agents de la police municipale avec le soutien de certains députés et députées, dont Patrick Hetzel (LR) ou encore Quentin Bataillon (Renaissance), essaient depuis 2018 d'avoir un accès direct* au fichier et non plus un accès indirect*.
Textes qui régissent ce fichier	- Arrêté du 7 juillet 2017 portant sur l'autorisation d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS) - Décision du Conseil n° 2007/533/JAI du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) - Loi n° 78-17 du 6 janvier 1978 modifiée 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 - Règlement (CE) n° 1987/2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II)
Sources	Voir ci-dessus « Textes qui régissent ce fichier » Amendement n°647 retiré, 13 novembre 2020 Bataillon Quentin, Question n°5824 « Accès des policiers municipaux aux fichiers (FOVes, FVA) » publiée au Journal officiel, 21 février 2023 Hetzel Patrick, « Policiers municipaux et accès aux fichiers », communiqué de presse, 26 octobre 2018

Nom du fichier	**FPR**
Sens de l'acronyme	Fichier des personnes recherchées
Date de création	15 mai 1996
Quelle échelle ?	Nationale
Objectifs officiels	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. Ce traitement a pour finalité de faciliter les recherches, les surveillances et les contrôles effectués dans le cadre des missions de police judiciaire et de police administrative. (Article 1 du décret n° 2010-569 du 28 mai 2010)
Objectifs implicites	Ce fichier est consulté lors de l'instruction de demandes de titres d'identité et de voyage, de visas et d'autorisations de voyage ainsi qu'à l'acquisition de la nationalité française. Le FPR, fichier à visée sécuritaire, participe aux contrôles grandissant des personnes étrangères et à la limitation de leur demande relative aux droits au séjour dans le cas d'un fichage. Ce fichier de police est lié au système d'information* Schengen, au niveau européen. Il limite la circulation et l'entrée sur le territoire au titre d'un fichage. D'autant plus qu'en France, le FPR et le N-SIS (voir fiche SIS II) sont systématiquement consultés par les policiers de la PAF. Or, comme constaté dans le cas de la fiche S, le fichage sur décision discrétionnaire est important dans le cadre du FPR. De plus, les possibilités de communication, de rectification et d'effacement des données peuvent être très compliquées dans le cadre du FPR. Le lien avec le SIS témoigne d'une « *extension des fichiers de sécurité publique* » selon Pierre Piazza (Pierre Piazza, « L'extension des fichiers de sécurité publique », 2009)
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'État - [PJ] recherche de police judiciaire 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 (par exemple, 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). Données contenues dans le FPR : - Identité de la personne recherchée (état civil, sexe, nationalité, adresse...) - Numéro national d'identification étranger, numéro de dossier du permis de conduire - Photographies et signes physiques distinctifs - Le motif de sa recherche et les actes (administratifs ou judiciaires) justifiant l'inscription de l'individu dans le fichier - La conduite à tenir en cas de découverte des personnes recherchées (Site de la Cnil sur le FPR et Article 3 du décret n° 2010-569 du 28 mai 2010)
Critères d'inscription dans ce fichier	Peuvent être inscrites dans le FPR : - Les personnes faisant l'objet des décisions judiciaires mentionnées à l'article 230-19 du code de procédure pénale ; - Les personnes faisant l'objet d'une recherche pour les besoins d'une enquête de police judiciaire. Peuvent également être inscrites (liste non exhaustive) : « *Les personnes de nationalité étrangère pour lesquelles il existe, eu égard aux informations recueillies, des éléments sérieux de nature à établir que leur présence en France constituerait une menace pour l'ordre public susceptible de justifier que l'accès au territoire français leur soit refusé* » ; - Les ressortissants et ressortissantes d'un État non-membre de l'Union européenne faisant l'objet d'une mesure restrictive de voyage, interdisant l'entrée sur le territoire ou le transit par le territoire, adoptée par l'Union européenne ou une autre organisation internationale et légalement applicable en France ; - Les personnes mineures faisant l'objet d'une opposition à la sortie du territoire ;

	- Les personnes mineures ayant quitté leur domicile ou s'étant soustraites à l'autorité des personnes qui en ont la garde ; - Les personnes faisant l'objet de recherches pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État, dès lors que des informations ou des indices réels ont été recueillis à leur égard ; - Les personnes qui font l'objet d'une mesure individuelle de contrôle administratif et de surveillance ; - Les personnes faisant l'objet de recherches en vue de la notification de mesures administratives concernant leur permis de conduire ; - Les personnes faisant l'objet d'une mesure administrative de retrait d'un permis de conduire obtenu indûment ; - Les personnes qui, au terme du délai prévu n'ont pas restitué au préfet du département de leur lieu de résidence, leur permis de conduire invalidé pour solde de points nul ; - Les personnes qui font l'objet d'une décision de retrait d'une carte nationale d'identité ou d'un passeport obtenu ou détenu indûment et celles qui ont tenté d'obtenir illégalement la délivrance d'une carte nationale d'identité ou d'un passeport ; - Les personnes étrangères faisant l'objet d'une OQTF non exécutée ; - Les personnes étrangères faisant l'objet d'une interdiction de retour et ceci pendant sa période de validité ; - Les personnes étrangères faisant l'objet d'une interdiction de circulation sur le territoire français et ceci pendant sa période de validité ; - Les personnes étrangères faisant l'objet d'un arrêté d'expulsion ; - Les personnes étrangères faisant l'objet d'une assignation à résidence ; - Les personnes qui font l'objet d'une décision d'interdiction de sortie du territoire ; - Les personnes auxquelles a été notifiée une décision d'interdiction de sortie du territoire et qui n'ont pas procédé à la restitution de leur passeport et de leur carte nationale d'identité dans le délai prévu ; - Les personnes étrangères qui font l'objet d'une interdiction administrative du territoire ; - Les personnes qui font l'objet d'une interdiction de séjour dans tout ou partie d'un département. **Précisions dans le cadre d'une fiche S** : « *Les personnes faisant l'objet de recherches pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État, dès lors que des informations ou des indices réels ont été recueillis à leur égard* » (Article 2, III, 8° du décret n° 2010-569). - 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. La loi étant particulièrement large à l'égard des critères de fichage S, l'éventail de motifs pour lesquels une personne peut se voir inscrite dans le fichier FPR avec une fiche S est également très large, et comprend à la fois des personnes recherchées par différents pays pour des activités terroristes, mais aussi des militants. En octobre 2023, Gérald Darmanin, alors ministre de l'intérieur, avait affirmé devant la Commission d'enquête de l'Assemblée nationale sur les groupuscules violents que des membres de « l'ultra-gauche » étaient fichés S. Par ailleurs, une personne liée à une personne fichée « S » peut aussi être fichée.
Autorité(s) compétente(s)	Direction générale de la police nationale et direction générale de la gendarmerie nationale (ministère de l'intérieur)
Qui a accès à ce fichier?	Peuvent avoir accès aux données enregistrées dans le FPR : - Les personnels de la police nationale individuellement désignés et spécialement habilités ; - Les personnels de la gendarmerie nationale individuellement désignés et spécialement habilités ; - Le personnel des services des douanes individuellement désigné et spécialement habilité ; - Le personnel des services centraux du ministère de l'intérieur et des préfectures et sous-préfectures individuellement désigné et spécialement habilité ; - Le personnel du ministère de l'Europe et des affaires étrangères, chargé du traitement des titres d'identité et de voyage et de l'instruction des demandes de visa, individuellement désigné et spécialement habilité ; - Le personnel du Conseil national des activités privées de sécurité, individuellement désigné et spécialement habilité ; - Le personnel de l'agence nationale des données de voyage individuellement désigné et spécialement habilité ; - Le personnel de la cellule de renseignement financier nationale ; - Le personnel du service national des enquêtes administratives de sécurité individuellement désigné et habilité ; - Le personnel du commandement spécialisé pour la sécurité nucléaire individuellement désigné et spécialement habilité ; - Le personnel du service national des enquêtes d'autorisation de voyage individuellement désigné et habilité ; - Le personnel du service central des armes et explosifs individuellement désigné et habilité ;

	- Le personnel des services spécialisés de renseignement du ministère des armées individuellement désigné et spécialement habilité ; - Le personnel du service national du renseignement pénitentiaire individuellement désigné et habilité ; - Les magistrates et magistrats du parquet, chargés de l'instruction et chargés de l'application des peines ; - Le personnel des services judiciaires, individuellement désigné et spécialement habilité ; - Les membres du personnel opérationnel du contingent permanent du corps européen de garde-frontières et de garde-côtes déployés dans le cadre des équipes affectées à la gestion des frontières extérieures, individuellement désignés et spécialement habilités ; - Le personnel affecté à l'Office français de la biodiversité, individuellement désigné et spécialement habilité. Peuvent être destinataires* des données enregistrées dans le FPR : - Les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers ; - Le personnel de la police municipale dans le cadre des recherches des personnes disparues : certaines informations peuvent être transmises oralement par les services de la police nationale et les unités de gendarmerie nationale au personnel de la police municipale en cas de « danger pour la population » ; - Le personnel du service gestionnaire du fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes ; - Le personnel du service gestionnaire du fichier judiciaire national automatisé des auteurs d'infractions terroristes. (Article 5 du décret n°2010-569 du 28 mai 2010) **Précision dans le cadre d'une fiche S** Les services de renseignement pouvant attribuer la qualification « S » à une personne fichée sont : - La Direction générale de la sécurité intérieure (DGSI) - Le Service central du renseignement territorial (SCRT) - La Direction du renseignement de la préfecture de police de Paris (DRPP) - La Direction générale de la gendarmerie nationale (DGGN)
Durée de conservation des données	- Les données à caractère personnel et informations enregistrées dans le fichier sont conservées jusqu'à l'aboutissement de la recherche ou l'extinction du motif de l'inscription. - À l'issue du délai fixé, les données à caractère personnel enregistrées dans le fichier sont conservées pendant une durée de 6 mois et accessibles uniquement aux personnels chargés de la création et de la gestion des fiches. - Les données à caractère personnel et informations relatives sont par la suite archivées pendant une durée de 6 ans. Elles sont uniquement accessibles aux personnels de la police nationale et aux personnels de la gendarmerie nationale chargés de l'administration du fichier des personnes recherchées. (Article 7 du décret n° 2010-569 du 28 mai 2010)
Échange de données	Le traitement FPR est interconnecté avec les fichiers suivants : N-SIS II (voir fiche SIS II), API-PNR, PARAFE[13], FIJAIT, AGDREF 2, LRPPN[14], LRGPN[15], les fichiers d'EUROPOL et les fichiers d'INTERPOL. - Les données stockées dans le fichier FPR peuvent être consultées depuis les fichiers ACCReD et SETRADER (Système européen de traitement des données d'enregistrement et de réservation).

[13] PARAFE (système de contrôle automatique aux frontières) : Il vise à accélérer le franchissement de frontières et donc à remplacer le contrôle humain, réalisé par des gardes-frontières, par une identification biométrique via un SAS automatique. Concrètement, il s'agit de scanner son passeport à l'entrée du SAS, puis de prendre position dedans : une caméra relève les traits du visage et confirme par la reconnaissance faciale l'identité du porteur ou de la porteuse du titre. Ce système est fondé sur la base du volontariat. Il n'a pas été inclus dans la boîte à fichiers car l'intérêt de PARAFE réside dans ses interconnexions avec le FPR, le SIS II et SLTD. PARAFE enregistre cependant l'image faciale, il est possible de s'y opposer. Cependant, la mention relative à la demande d'effacement des données n'est pas inscrite dans la législation. Pour les informations complémentaires, voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 135.

[14] LRPPN (Logiciel de Rédaction des Procédures de la Police Nationale) alimente automatiquement le TAJ, FOVeS et CASSIOPEE, et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer au vu de sa proximité avec le TAJ et le FAED. Pour les informations complémentaires, voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

[15] LRPGN (Logiciel de Rédaction des Procédures de la Gendarmerie Nationale) alimente automatiquement le TAJ, FOVeS et CASSIOPEE, et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer au vu de sa proximité avec le TAJ et le FAED. Pour les informations complémentaires, voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

Comment obtenir communication et rectification des données ?	Le droit d'opposition* n'est pas applicable. Le droit d'accès est direct pour : - Les personnes inscrites pour des raisons n'intéressant par la sûreté de l'État (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'État - 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* *Ou via le téléservice : Plateforme numérique des demandes de droit d'accès au fichier des personnes recherchées (autre que celles intéressant la sûreté de l'État) · demarches-simplifiees.fr* - Le modèle de courrier concernant le **droit d'accès** Les modèles de courrier concernant le **droit de rectification** : - lorsque les données sont incomplètes - lorsque les données sont inexactes Disponible sur le site de la Cnil « FPR » **Pour la fiche S** Contrairement aux autres catégories du FPR, les demandes relatives aux droits d'accès, de rectification et d'effacement des données dans les fiches S doivent être adressées à la Cnil. Les données peuvent être communiquées à la personne requérante si la Cnil considère que cela ne met pas « en cause » les finalités du traitement, « la sûreté de l'État, la défense ou la sécurité publique », conformément à l'article 118 de la loi n° 78-17 du 6 janvier 1978. (Article 9 du décret n° 2010-569)
Remarques	Depuis 2015, toute personne étant sous le coup d'une obligation de quitter le territoire français (OQTF) est automatiquement enregistrée dans le fichier FPR.
Textes qui régissent ce fichier	- Article 230-19 du code de procédure pénale - Articles L. 231-4 à L. 231-5 du code des relations entre le public et l'administration - Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées - Décret n° 2017-1219 du 2 août 2017 modifiant le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées - Décret n° 2023-979 du 23 octobre 2023 modifiant le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées - Délibération de la Cnil n° 88-120 du 8 novembre 1988 de la Cnil 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 - Délibération n° 92-056 du 9 juin 1992 de la Cnil 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 - Délibération n° 95-051 du 25 avril 1995 de la Cnil 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* - Délibération n° 2006-292 du 21 décembre 2006 de la Cnil portant avis sur le projet d'arrêté portant modification de l'arrêté du 15 mai 1996 modifié relatif au fichier des personnes recherchées - Délibération n° 2009-587 du 12 novembre 2009 de la Cnil portant avis sur un projet de décret en Conseil d'État relatif au fichier des personnes recherchées (FPR) - 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

	- 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 Cnil, « FPR : Fichier des personnes recherchées », 2009 Cotteret Jean-Marie, Rapport de recherche n°2 « Les fichiers de police et de renseignement en France », Centre Français de Recherche sur le Renseignement, 2017 David Romain, « Fiché « S », FPR, FSPRT… quels sont les différents fichiers de renseignement utilisés pour la lutte antiterroriste ? », Public Sénat, 16 octobre 2023 Januel Pierre, « L'Intérieur muscle le fichier des personnes recherchées », Next, 2023 Piazza Pierre, « L'extension des fichiers de sécurité publique », *Revue Hermes*, n° 53, 2009 Sénat, « Les fiches S en questions : réponses aux idées reçues », Rapport d'information n°219 (2018-2019), 19 décembre 2018

Nom du fichier	**France-Visas**
Date de création	26 septembre 2017 Déploiement dans le réseau consulaire depuis la fin mai 2023
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectif de : - Permettre d'effectuer des demandes de visa en ligne ; - Mettre à la disposition des entreprises et institutions habilitées, un espace de dépôt d'invitation en faveur de leurs partenaires étrangers soumis à l'obligation de visa ; - Traiter les demandes de visas, notamment grâce à l'échange d'informations avec les autorités nationales et les autorités des États mettant en œuvre l'acquis de Schengen ; - Lutter contre l'entrée et le séjour irréguliers des étrangers en France, en prévenant les fraudes documentaires, les usurpations d'identité et les détournements de procédure.
Objectif implicite	France-Visas permet le renforcement du contrôle aux frontières extérieures l'UE et au sein du territoire français. Ce fichier centralise les informations pour surveiller les personnes dans le cadre de leur demande de visa et de vérifier qu'elles respectent la durée de leur visa, ainsi que les sorties du territoire. Enfin, son objectif de « *lutte contre l'entrée et le séjour irrégulier* » en fait un fichier de police et de contrôle des personnes étrangères.
Contenu des données	Les données relatives : - À la personne demandeuse de visas elle-même (données d'identification, données relatives au document de voyage et au titre de séjour) ; - À la personne déposant la demande, si elle est différente de la personne demandeuse ; - À la demande de visa (données relatives à la demande elle-même, données spécifiques relatives à certaines catégories de visas, données relatives aux précédents séjours, données relatives aux répondants) ; - Au traitement de la demande de visa (données relatives à la consultation* par France-Visas des partenaires Schengen, des services tiers et à la consultation* des traitements FPR, SIS II et EES, données relatives à l'instruction de la demande et à la perception des droits de timbre, données relatives à la décision) ; - Aux procédures d'attention et d'authentification des actes d'état civil. (Article R. 142-60 du CESEDA) Les données sont listées à l'annexe 11 du CESEDA Les données enregistrées dans le traitement peuvent faire apparaître, directement ou indirectement, « *des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques*, des données biométriques* aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ». Les opérations de collecte, modification, consultation, communication, interconnexion et effacement des données contenues dans le traitement France-Visas doivent faire l'objet d'un enregistrement.

	(Article R. 142-65 du CESEDA)
Critères d'inscription dans ce fichier	Toute personne effectuant une demande de visa pour entrer sur le territoire français ou en situation de transit aéroportuaire.
Autorité(s) compétente(s)	Ministres de l'intérieur et des affaires étrangères
Qui a accès à ce fichier ?	Ont accès aux données collectées à raison de leurs attributions et dans la limite du besoin d'en connaître : - Le personnel des services centraux du ministère de l'intérieur, du ministère de l'Europe et des affaires étrangères et du ministère chargé des douanes participant à l'instruction des demandes de visas ; - Le personnel des missions diplomatiques et des postes consulaires chargé de l'instruction des demandes de visas ; - Le personnel des préfectures chargé de l'instruction des demandes de visas et de l'application de la réglementation relative à la délivrance des titres de séjour, au traitement des demandes d'asile et à la préparation et à la mise en œuvre des mesures d'éloignement ; - Le personnel de la police nationale, le personnel des services des douanes et le personnel de la gendarmerie nationale chargé de l'instruction des demandes de délivrance de visas aux frontières et des vérifications aux frontières extérieures des documents de voyage des ressortissants des pays tiers ; - Le personnel des prestataires de services extérieurs chargé de la vérification de la complétude des dossiers de demande de visas, ainsi que de la prise de biométries le cas échéant, avant transmission du dossier au poste consulaire pour instruction. (Article R. 142-61 du CESEDA) L'ensemble de ce personnel est habilité à collecter les données renseignées dans le traitement, en respectant le niveau de protection et les garanties équivalentes à celles du droit français (Article R. 142-62 du CESEDA). Le personnel pouvant être destinataire des données collectées dans le traitement France-Visas sont : - Le personnel des services du ministère de l'intérieur (direction nationale de la police aux frontières, direction du renseignement de la préfecture de police et direction générale de la sécurité intérieure) individuellement désigné et habilité par leur autorité hiérarchique ; - Le personnel des services du ministère des armées (direction générale de la sécurité extérieure, direction du renseignement et de la sécurité de la défense, direction du renseignement militaire) individuellement désigné et habilité par leur autorité hiérarchique ; - Le personnel des services centraux du ministère de l'intérieur, du ministère de l'Europe et des affaires étrangères et du ministère chargé des douanes participant à la gestion des recours administratifs et contentieux dirigés contre les décisions prises en matière de visas, individuellement désigné et habilité par leur autorité hiérarchique ; - Le personnel des organismes de sécurité sociale, dans le cadre de leur mission de lutte contre la fraude, individuellement désigné et habilité par leur autorité hiérarchique. (Article R. 142-63 du CESEDA)
Durée de conservation des données	- Les données renseignées dans le traitement France-Visas sont conservées durant une durée maximale de 5 ans à compter de la date de délivrance, de refus, de réduction, de prorogation ou d'abrogation du visa ou de la date de la création du dossier de demande de visa en cas de clôture ou d'interruption de la demande. - Les empreintes digitales enregistrées dans le traitement sont conservées pendant une durée maximale d'1 mois à compter de la date de délivrance ou de refus de visa lorsqu'elles sont rattachées à une demande de visa, ou une durée maximale d'1 mois à compter de la date de leur collecte lorsqu'elles ne sont pas rattachées à une demande de visa. - Les identifiants et mots de passe associés aux comptes utilisateur de l'application* France-Visas ainsi que l'identité, la dénomination ou la raison sociale de la personne demandeuse de visa sont effacées au bout d'un an en cas d'inactivité du compte de manière ininterrompue, après information du titulaire. - Les données issues des systèmes SIS et FPR sont conservées pendant une durée maximale de 50 jours, à l'exclusion du numéro d'enregistrement de la personne ou du document de voyage issu de ces systèmes (qui est enregistré selon les durées de conservation du FPR et du SIS II). - Les données issues du système EES sont conservées pendant une durée maximale de 100 jours à compter de la date de délivrance, de refus, de réduction, de prorogation ou d'abrogation du visa ou de la date de la création du dossier de demande de visa en cas de clôture ou d'interruption de la demande. - Les données relatives aux procédures d'attention et d'authentification des actes d'état civil sont conservées durant une durée maximale de 5 ans à compter de la date d'ouverture de la procédure lorsqu'elles ne font pas l'objet d'un rattachement à une demande de visa, ou à compter de la date de délivrance, de refus, de réduction ou de prorogation du visa lorsqu'elles font l'objet d'un tel rattachement. - Les données enregistrées au titre des demandes en ligne incomplètes sont conservées pendant une durée de 3 mois à compter de la dernière modification du dossier de demande. (Article R. 142-64 du CESEDA)

	Les données relatives aux opérations menées autour de ces données (de collecte, de modification, de consultation, de communication, d'interconnexion et d'effacement des données) sont conservées durant trois ans. (Article R. 142-65 du CESEDA)
Échanges de données	France-Visas est le traitement national avec VISABIO permettant l'accès au fichier européen VIS. L'interconnexion avec le fichier des documents de voyage volés ou perdus d'INTERPOL n'est pas mentionnée par le décret n° 2024-810 créant l'annexe 11 du CESEDA. L'annexe 11 du CESEDA indique que le traitement France-Visas consulte automatiquement le N-SIS (voir fiche SIS II), EES, AGDREF 2, FPR. Une communication automatique de données à caractère personnel renseignées dans le traitement France-Visas vers le traitement VISABIO est prévue. Les données communiquées sont listées à l'annexe 2 du CESEDA.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas (Article R. 142-68 du CESEDA). Les droits d'accès, de rectification et à la limitation s'exercent auprès de l'autorité de délivrance du visa (Article R. 142-66 du CESEDA). Les droits d'accès et de rectification peuvent faire l'objet de restrictions à des fins de sauvegarde de la sécurité nationale, de protection contre les menaces pour la sécurité publique et de prévention de telles menaces. Les personnes concernées par de telles restrictions peuvent exercer leurs droits auprès de la Cnil (Article R. 142-67 du CESEDA).
Remarques	Le traitement France-Visas remplace le fichier RMV 2, démantelé à cause de manquements à la législation européenne. En 2021, la plateforme France-Visas a été victime d'une attaque informatique au cours de laquelle des données personnelles ont été dérobées (Next, 2024 ; Next, 2021).
Textes qui régissent ce fichier	- Annexes 2 et 11 du CESEDA - Articles R. 142-59 à R. 142-68 du CESEDA - Arrêté du 26 septembre 2017 portant création d'un traitement automatisé de données à caractère personnel relatif aux étrangers sollicitant la délivrance d'un visa - Abrogé par décret n°2024-810 du 6 juillet 2024 relatif au traitement de données* à caractère personnel relatif aux étrangers sollicitant la délivrance d'un visa
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Clavey Martin, « Jusqu'en 2023, le système français d'accès aux données de demandes de visas Schengen était dans l'illégalité », Next, 1er février 2024 Gavois Sébastien, « Fuite de données personnelles sur la plateforme France-visas », Next, 7 septembre 2021

Nom du fichier	**RMV 2 - Remplacé par France-Visas**
Sens de l'acronyme	Réseau Mondial Visa 2 Le fichier RMV 2 a remplacé le fichier RMV. Il est aujourd'hui remplacé par France-Visa.
Date de création	22 août 2001
Quelle échelle ?	Nationale
Raison du démantèlement	En 2023, et après plusieurs opérations de contrôle menées depuis 2020, la Cnil a conclu que le traitement RMV 2 fonctionnait de manière illicite et a prononcé un rappel à l'ordre à l'encontre des ministères des affaires étrangères et de l'intérieur. Le système RMV 2 consultait systématiquement les traitements SIS et VIS lorsqu'une demande de visa était déposée. Ce processus impliquait la création de copies des données enregistrées dans le traitement N-SIS français vers le traitement RMV 2, dans un objectif de gestion des procédures de délivrance de visa et de « *contrôles sécuritaires* ». Ces copies étaient non seulement enregistrées dans le système central du RMV 2, mais également dans les 157 systèmes locaux dans les postes consulaires, et conservées pour des durées dépassant 48 heures. Or, la création de ces copies était contraire à la législation européenne. L'article 31 du règlement (CE) n° 1987/2006 du Parlement européen et du Conseil et l'article 41 du règlement (UE) 2018/1861 du Parlement européen et du Conseil disposent que les données du traitement SIS ne peuvent être copiées qu'à des fins techniques, lorsque cela est nécessaire aux autorités compétentes pour effectuer une recherche, et leur conservation ne peut dépasser 48 heures. En outre, la Cnil a soulevé que le recours à des copies est proscrit par le règlement (CE) n° 767/2008 du Parlement européen et du Conseil lorsque les autorités sont reliées au système VIS. Or, le ministère de l'Europe et des affaires étrangères et les postes consulaires sont reliés au système VIS et ont procédé à des copies. Par ailleurs, la Cnil a relevé que ces pratiques de copies pouvaient mener à des erreurs et ne permettaient pas de garantir l'exactitude des données, ce qui va à l'encontre de l'article 4 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Enfin, contrairement aux dispositions des articles 12 des règlements n° 1987/2006 et n° 2018/1861 et aux exigences des articles 32 2. i) et 34 du règlement n° 2008/767, aucune journalisation* des accès à la copie locale du N-SIS n'a été mise en place, ce qui va à l'encontre des exigences de sécurité des traitements.
Traitement des données enregistrées après le démantèlement	L'article 4 du décret n° 2024-810 du 6 juillet 2024 relatif au traitement de données* à caractère personnel relatif aux étrangers sollicitant la délivrance d'un visa dénommé France-Visas abroge l'arrêté du 22 août 2001 portant création du traitement RMV2 et précise que le ministre de l'intérieur et le ministre des affaires étrangères « *sont autorisés à utiliser les données enregistrées dans ces traitements jusqu'au terme de la durée de conservation qui en était fixée par ces arrêtés, aux fins qu'ils autorisaient* », soit durant une durée maximale de 5 ans.
Objectifs officiels	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 parties à la Convention 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.

	Cette consultation* permet de savoir si le demandeur est signalé dans une des autres bases de données auxquelles donne accès le réseau. (Gérard Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs », 2008)
Objectifs implicites	Opérer un contrôle accru des personnes étrangères en croisant les fichiers des différentes demandes d'entrée 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 et commerçante - 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... (Annexe 6-3 du CESEDA)
Critères d'inscription dans ce fichier	Personne demandeuse de visa
Autorité(s) compétente(s)	Le ministère de l'Europe et des affaires étrangères, le ministère de l'intérieur et les autorités centrales des pays Schengen dans la limite de leurs attributions
Textes qui régissent ce fichier	- 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 - 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 - Décret n° 2024-810 du 6 juillet 2024 relatif au traitement de données* à caractère personnel relatif aux étrangers sollicitant la délivrance d'un visa dénommé France-Visas - Délibération n°SAN-2023-017 du 11 décembre 2023 de la Cnil - 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 - 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)
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Clavey Martin, « Jusqu'en 2023, le système français d'accès aux données de demandes de visas Schengen était dans l'illégalité », Next, 2024 Dubey Gérard, « Nouvelles techniques d'identification, nouveaux pouvoirs », cahiers internationaux de sociologie, n° 125, 2008 La Cimade, *Visa refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas*, Rapport d'observation, 2010 Lochak Danièle, « Des fichiers pour gérer, contrôler et surveiller les étrangers », Plein droit, n° 71, 2006

Nom du fichier	**FSPRT**
Sens de l'acronyme	Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste
Date de création	Avril 2015
Quelle échelle ?	Nationale
Objectifs officiels	L'objectif de ce fichier est la centralisation des « *informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste, en vue de l'information des autorités compétentes et de leur exploitation par les services et du suivi des personnes concernées* ». Il permet le suivi des signalements effectués par le centre national d'assistance et de prévention de la radicalisation (CNAPR) ou des préfectures. L'analyse des données récoltées dans ce fichier sert également à la réflexion autour de nouvelles politiques publiques « *de lutte contre la radicalisation* ». (Assemblée Nationale, Rapport d'information n° 1335, 17 octobre 2018)
Objectif implicite	Surveillance massive des personnes, basée sur des critères qui ne sont pas clairement définis et qui sont interprétés de manière large.
Contenu des données	Information non publique. Le fichier contiendrait, entre autres, l'identité de la personne fichée, sa localisation, ses antécédents judiciaires, sa situation psychiatrique le cas échéant (Cf2R, 2017).
Critères d'inscription dans ce fichier	Une personne est inscrite dans le fichier FSPRT lorsqu'elle a fait l'objet d'un signalement par les préfectures, par le CNAPR ou par les services de police et de gendarmerie. La CNAPR est une plateforme téléphonique accessible gratuitement afin de signaler la radicalisation d'un proche. Les personnes administrant cette plateforme ont à leur disposition des indicateurs leur permettant d'identifier les situations de radicalisation. Ces indicateurs ont été créés par un groupe de travail piloté par le Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation (SG-CIPDR). Ce groupe de travail est constitué d'acteurs et actrices diverses incluant les ministères de l'intérieur, de la justice, de l'éducation nationale, des affaires sociales et de la santé, de la ville, de la jeunesse et des sports et la mission interministérielle de vigilance et de lutte contre les dérives sectaires (CNCDH, 2018).
Autorité(s) compétente(s)	Direction générale de la sécurité intérieure (ministère de l'intérieur)
Qui a accès à ce fichier ?	Le suivi des personnes fichées peut dépendre de différents services, incluant la direction générale de la sécurité intérieure (DGSI), le service central du renseignement territorial (SCRT) et la direction du renseignement de la Préfecture de police de Paris (DRPP). Ces données sont évaluées par les groupes d'évaluation départementaux de la radicalisation (GED). Le service affecté dépend de la « dangerosité » évaluée de la personne fichée, la DGSI étant le service en charge du suivi des personnes considérées comme les plus « dangereuses ». Dans le cadre d'enquêtes administratives, le service national des enquêtes administratives de sécurité (SNEAS) et le commandement spécialisé pour la sécurité nucléaire (COSSEN) peuvent, via l'application* ACCReD, consulter le fichier FSPRT (Assemblée nationale, Rapport d'information n° 1335, 17 octobre 2018)
Durée de conservation des données	Selon la Caisse de solidarité de Lyon, « *Les données sont conservées pendant 5 ans, mais un membre du Conseil de la fonction militaire de la gendarmerie a reconnu que les « informations ne sont pas perdues ensuite*[16] *»* ».
Échanges de données	En vertu du décret n° 2019-412, le fichier FSPRT est interconnecté avec le fichier HOPSYWEB[17] qui permet le traitement de données* à caractère personnel relatif au suivi des personnes en soins psychiatriques sans consentement.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. L'exercice des droits d'accès et de rectification est indirect : il faut passer par la Cnil.
Remarques	Dans son avis sur la prévention de la radicalisation, publié au Journal officiel le 1er avril 2018, la Commission nationale consultative des droits de l'Homme (CNCDH) souligne « *l'absence de cohérence des profils réunis au sein du fichier FSPRT, au regard de l'objectif sécuritaire qui lui est assigné* ». Elle indique que « [*l*]*es personnes fichées ne font pas toutes l'objet d'un signalement en raison d'agissements menaçants, directement ou indirectement, la sûreté de l'État mais simplement en raison d'une conduite ou d'un comportement exprimant une conviction politique ou religieuse* ». En octobre 2023, Gérald Darmanin, Ministre de l'intérieur, déclarait que 193 personnes étrangères en situation irrégulière inscrites dans le fichier FSPRT devaient faire l'objet « *d'une expulsion systématique* » (Public Sénat, 16 octobre 2023).
Textes qui régissent ce fichier	- Le fichier a été créé par le décret n° 2015-252 du 4 mars 2015 puis modifié à plusieurs reprises (décrets du 30 octobre 2015, du 2 août 2017, du 15 mars 2021 et du 29 novembre 2023). Aucun de ces décrets n'a été rendu public.

[16] Fenech G., Pietrasanta S., Rapport d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015, Rapport n° 3922, Assemblée nationale, 2016.
[17] Le fichier HOPSYWEB est un fichier sanitaire recensant les données relatives aux personnes faisant l'objet de mesures de soins psychiatriques sans consentement. Il est devenu, du fait de son interconnexion avec le FSPRT, un fichier de police. Il n'a pas été détaillé dans le cadre de cette boîte à fichiers. Pour plus d'informations, voir Mathias Couturier, « Hopsyweb : d'un fichier sanitaire à un fichier policier ? », *Cahiers de la recherche sur les droits fondamentaux*, n° 21, 2023.

	- 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Assemblée nationale, Rapport d'information n° 1335, 2018 Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 CNCDH, avis sur la prévention de la radicalisation, 2018

Nom du fichier	**GESI**
Sens de l'acronyme	Gestion des étrangers en situation irrégulière
Date de création	21 septembre 2011
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectif de : - Assurer la gestion des dossiers en temps réel, de l'interpellation jusqu'à la reconduite à la frontière, des personnes étrangères en situation irrégulière interpellés par les services de la préfecture de police ; - Exploitation des données contenues à des fins de recherches statistiques. (Article 1 de l'arrêté du 21 septembre 2011 portant création du GESI)
Objectif implicite	Le fichier GESI, avec le fichier GIPI, remplace l'ancien fichier de gestion des personnes étrangères non-admises sur le territoire français (le FNAD, « fichier des non-admis », abrogé en 2012). Le fichier GESI est un outil opérationnel de police judiciaire à la disposition des agents de ce service, leur permettant d'assurer un suivi en temps réel des procédures judiciaires en cours. En conséquence, selon la Cnil « *il a pour objectif la constatation et la poursuite d'infractions pénales* ». Le fichier GESI permet l'identification, le contrôle et le suivi des procédures judiciaires relatives aux personnes étrangères en situation dite irrégulière : de leur interpellation par les services compétents de la préfecture de police à l'exécution de l'éventuelle mesure d'éloignement décidée à leur encontre. De plus, le fichier GESI a pour objectif de produire des données statistiques (nombre de personnes interpellées par département, par âge, par nationalité, etc., nombre de personnes placées en garde à vue, faisant l'objet de poursuites pénales, etc.), émanant de demandes des autorités ministérielles, du cabinet du préfet de police ou du directeur du renseignement. Délibération n° 2011-175 du 16 juin 2011 de la Cnil portant avis sur un projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé « gestion des étrangers en situation irrégulière » (GESI) (demande d'avis n° 1435785)
Contenu des données	Les catégories de données à caractère personnel enregistrées sont celles relatives : - À l'identité de la personne étrangère (nom, prénom, âge, date et lieu de naissance, nationalité, sexe) - Au numéro de dossier AGDREF (gestion informatisée des dossiers de ressortissants étrangers en France) - Au service interpellateur - Aux données relatives aux procédures judiciaires en cours - Au domicile d'assignation à résidence - Aux coordonnées du vol de retour du reconduit (Article 2 de l'arrêté du 21 septembre 2011)
Critères d'inscription dans ce fichier	Personne étrangère en situation irrégulière interpellée par les services compétents de la préfecture de police et en cours de procédure judiciaire ou administrative
Autorité(s) compétente(s)	Le ou la préfète de police, service chargé de la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la direction du renseignement
Qui a accès à ce fichier ?	Ont accès à ce fichier les officiers, officières, agents et agentes de police judiciaire affectés au service chargé de la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la direction du renseignement de la préfecture de police, individuellement désignés et spécialement habilités par le ou la préfète de police.

	Il a été déclaré à la Cnil que les données seront uniquement accessibles sur le réseau interne de la préfecture de police. Peuvent être destinataires* des données : - Les officiers, officières, agents et agentes de police judiciaire des direction et services actifs de la préfecture de police ayant procédé aux opérations prévues au chapitre III du titre II du livre Ier du code de procédure pénale, - Les agents et agentes de la police nationale affectés à la direction de l'ordre public et de la circulation de la préfecture de police chargés des opérations de transfert des personnes étrangères en situation irrégulière - Les agents et agentes de la direction de la préfecture de police chargée de la police des étrangers - Les magistrats et magistrates du parquet et de l'instruction
Durée de conservation des données	3 mois à partir de la date du dernier fait enregistré pour une même affaire. (Article 3 de l'arrêté du 21 septembre 2011)
Échanges de données	Le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration a mentionné à la Cnil que le traitement GESI ne fera l'objet d'aucune mise en relation, rapprochement* ou interconnexion avec un autre fichier. Voir dernier paragraphe de la délibération n° 2011-175 du 16 juin 2011 de la Cnil portant avis sur un projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé « gestion des étrangers en situation irrégulière » (GESI).
Quelle échelle ?	Nationale
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration a déclaré à la Cnil que les personnes sont informées oralement par les fonctionnaires de police, lors de la garde à vue, de l'enregistrement de leurs données personnelles dans le traitement GESI. Et que cette information sera complétée par une affiche apposée dans les salles d'audition, qui mentionnera les modalités d'exercice des droits d'accès et de rectification aux données qui les concernent. Les droits d'accès et de rectification s'exercent de manière indirecte auprès de la Cnil dans les conditions prévues aux articles 41 et 42 de la loi n° 78-17 du 6 janvier 1978. (Article 5 et Article 6 de l'arrêté du 21 septembre 2011)
Remarques	La Cnil soulignait que « *s'agissant de ces deux dernières catégories de données [données liées au domicile d'assignation à résidence ; et données liées aux coordonnées du vol de retour du reconduit], la commission relève qu'elles ne pourront être enregistrées dans le traitement GESI que dans le cas où elles concernent des ressortissants étrangers ayant fait l'objet d'une mesure d'éloignement décidée par l'autorité administrative compétente. Elle prend donc acte que la rédaction de l'article 2 du projet d'arrêté sera modifiée sur ce point* ». **Or, il n'y a pas de précision spécifique sur ce point dans l'arrêté du 21 septembre 2011 portant création du GESI**. Enfin, dans son avis elle relève « *que la préfecture de police n'a pas prévu de système de gestion des habilitations pour l'accès au traitement GESI, de sorte que chaque utilisateur du système aura accès, en lecture et en modification, à l'intégralité des données. Compte tenu de l'échelle réduite du traitement et du faible nombre d'utilisateurs, la commission considère que cette absence de gestion des habilitations n'est pas contraire aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée, sous réserve cependant que la sécurité de ces accès soit mieux assurée.* *En effet, elle observe que ces accès seront conditionnés à la fourniture de mots de passe de six caractères minimum, contenant des lettres et des chiffres, mais sans durée de validité. Ces modalités d'accès n'apparaissent pas suffisantes au regard des obligations de sécurité incombant au responsable du traitement. La commission demande donc que la préfecture de police prévoit l'utilisation de mots de passe de huit caractères, contenant des lettres en majuscule et en minuscule ainsi que des chiffres et des caractères spéciaux, qui soient valables pour une durée limitée, de trois mois par exemple* ». (Cnil, Délibération n° 2011-175 du 16 juin 2011)
Textes qui régissent ce fichier	- Arrêté du 21 septembre 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé « gestion des étrangers en situation irrégulière » (GESI) - Délibération n° 2011-175 du 16 juin 2011 de la Cnil portant avis sur un projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé « gestion des étrangers en situation irrégulière » (GESI) (demande d'avis n° 1435785) - Article R. 15-19 et chapitre III du titre II du livre Ier du code de procédure pénale - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier »

Nom du fichier	**GESTEL**
Sens de l'acronyme	Gestion de l'éloignement
Date de création	7 février 2019
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectif de : - Assurer la gestion de la mise en œuvre opérationnelle, matérielle et logistique des mesures d'éloignement, au sein de la direction nationale de la police aux frontières et des services territoriaux de la police nationale chargés de la police aux frontières ; - Améliorer l'exécution des mesures d'éloignement par la dématérialisation des échanges d'informations externes et internes ; - Garantir le suivi des procédures d'éloignement et d'en faciliter le contrôle. (Article R. 142-26 du CESEDA) Le ministère a indiqué à la Cnil l'utilité du fichier pour produire des statistiques concernant l'activité du service (nombre de saisines par préfecture, nombre d'annulations, nombre d'individus ayant été refoulés, nombre de programmations avec escorte). (Cnil, Délibération n° 2018-162 du 17 mai 2018)
Objectifs implicites	Ce fichier participe à l'identification, au contrôle et à l'éloignement des personnes n'étant pas - au moment du contrôle – régularisées. Il facilite la mise en œuvre d'une mesure d'expulsion, obligation de quitter le territoire Français, signalement aux fins de non-admission, arrêté de reconduite à la frontière, interdiction judiciaire ou administrative du territoire. Parmi ces mesures, plusieurs impliquent un départ forcé de l'étranger/étrangère ou s'accompagnent de mesures privatives de liberté.
Contenu des données	- Données relatives au service à l'origine de la demande de réacheminement, transfert ou refoulement : préfecture, numéro de dossier, date et heure de saisine, etc. - Données relatives à l'état civil de la personne ressortissante étrangère faisant l'objet de la mesure d'éloignement : numéro AGDREF, nom, prénoms, nationalité, etc. - Données relatives à la situation administrative de la personne ressortissante étrangère faisant l'objet de la mesure d'éloignement : décisions administratives (OQTF, interdiction du territoire français (ITF), etc.), documents d'identité, etc. - Données relatives à la requête de la demande de réacheminement, transfert ou refoulement : destination (pays et ville), vecteur souhaité pour le transport, date sollicitée… - Renseignements complémentaires : escorte, personnes accompagnantes, refus antérieurs d'embarquer - Données relatives aux itinéraires empruntés et les réservations hôtelières : nom du transporteur, jour et heure de départ et d'arrivée, etc. - Données relatives aux documents numérisés relatifs à la personne concernée par la mesure de réacheminement, transfert ou refoulement : fiche pénale, accord de réadmission, main courante, certificats médicaux, etc. Liste exhaustive des données à l'annexe 4 du CESEDA
Critères d'inscription dans ce fichier	Personne faisant l'objet d'une mesure d'éloignement
Autorité(s) compétente(s)	La direction générale de la police nationale (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont accès à ce fichier, les membres du personnel individuellement désignés et spécialement habilités : - De la direction nationale de la police aux frontières (PAF) et les services territoriaux de la PAF ; - Des préfectures de département et de la préfecture de police (Article R.142-28 du CESEDA) Peuvent être destinataires* des données : - Le ou la contrôleuse générale des lieux de privation de liberté ; - Les agents et agentes et militaires de la direction générale de la gendarmerie nationale ; - Les agents et agentes de la direction générale de la police nationale ; - Les agents et agentes de la direction générale des douanes et droits indirects ; - Les agents et agentes de la direction générale des étrangers en France ; - Les prestataires voyagistes agréés 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. 142-29 du CESEDA)
Durée de conservation des données	- Pendant une durée de 2 ans à compter de la date de leur enregistrement pour permettre l'exécution de la mesure de réacheminement, transfert ou refoulement. - Pendant une durée de 6 mois après la date d'exécution effective de la mesure de réacheminement, transfert ou refoulement.

	Les données à caractère personnel et informations relatives aux personnes dont la mesure de réacheminement, transfert ou refoulement 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. À l'issue de ces délais, ces données à caractère personnel et informations sont conservées pendant une durée de 6 ans et uniquement accessibles aux agents et agentes relevant de la cellule opérationnelle de l'éloignement de la direction centrale de la police aux frontières. (Article R. 142-30 du CESEDA)
Échanges de données	Pas d'interconnexion avec des fichiers
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'information, d'accès, de rectification, d'effacement et à la limitation s'exercent auprès de la direction générale de la police nationale. (Article R. 142-32 du CESEDA)
Remarques	Dans la délibération n° 2018-167 du 17 mai 2018 de la Cnil, la commission « estime dès lors 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 et que l'annexe précitée du CESEDA soit modifiée en ce sens ». Or, ces données ont été maintenues dans le traitement AGDREF 2 comme mentionnée à l'annexe 3 du CESEDA.
Textes qui régissent ce fichier	- Articles R. 142-26 à R. 142-32 et annexe 4 du CESEDA - 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 CESEDA - Décret n° 2023-1013 du 2 novembre 2023 relatif aux services déconcentrés et à l'organisation de la police nationale - Délibération n° 2018-162 du 17 mai 2018 de la Cnil portant avis sur un projet de décret autorisant un traitement automatisé de données à caractère personnel dénommé « Gestion de l'éloignement » - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier »

Nom du fichier	**GIPASP**
Sens de l'acronyme	Gestion de l'information et prévention des atteintes à la sécurité publique
Date de création	29 mars 2011
Quelle échelle ?	Nationale
Objectifs officiels	Le fichier GIPASP a pour finalité de « *recueillir, de conserver et d'analyser les informations qui concernent des personnes physiques ou morales ainsi que des groupements dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'État* ». (Article R. 236-21 du code de la sécurité intérieure)
Objectif implicite	Ce traitement permet le fichage massif de militantes et militants politiques, de leur entourage (notamment de leurs enfants mineurs), incluant des informations sur leur santé ou leurs activités sur les réseaux sociaux.
Contenu des données	Données concernant la personne physique pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État : - Éléments d'identification : nom, prénoms, alias, date et lieu de naissance, nationalité, signes physiques particuliers et objectifs, photographies, documents d'identité (type, numéro, validité, autorité et lieu de délivrance), origine géographique (lieux de résidence et zones d'activité) - Coordonnées : numéros de téléphone, adresses postales et électroniques, identifiants utilisés (pseudonymes, sites ou réseaux concernés, autres identifiants techniques), à l'exclusion des mots de passe, adresses et lieux fréquentés - Situation : situation familiale, formation et compétences, profession et emplois occupés, moyens de déplacement (moyens utilisés, immatriculation des véhicules, permis de conduire), situation au regard de la réglementation de l'entrée et du séjour en France, éléments patrimoniaux - Motifs de l'enregistrement - Activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État : activités publiques ou au sein de groupements ou de personnes morales, comportement et habitudes de vie, déplacements, activités sur les réseaux sociaux, pratiques sportives, pratique et comportement religieux

	- Facteurs de dangerosité : lien avec des groupes extrémistes, éléments ou signes de radicalisation, suivi pour radicalisation, données relatives au troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur, armes et titres afférents, détention d'animaux dangereux, agissements susceptibles de recevoir une qualification pénale, antécédents judiciaires (nature des faits et date), fiches de recherche, suites judiciaires, mesures d'incarcération (lieu, durée et modalités), accès à des zones ou des informations sensibles - Facteurs de fragilité : facteurs familiaux, sociaux et économiques, régime de protection, faits dont la personne a été victime, comportement auto-agressif, addictions, mesures administratives ou judiciaires restrictives de droits, décidées ou proposées Données concernant les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne pouvant porter atteinte à la sécurité publique ou la sûreté de l'État, notamment ses parents et ses enfants, dans la stricte mesure où ces données sont nécessaires pour son suivi et dans la limite des catégories mentionnées dans l'article R. 236-22 du code de la sécurité intérieure. Données concernant les victimes des agissements de la personne physique pouvant porter atteinte à la sécurité publique ou la sûreté de l'État, dans les conditions renseignées à l'article R. 236-22 du code de la sécurité intérieure. Données concernant les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne morale ou le groupement pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État, ou victimes des agissements de ces personnes morales et groupements, dans les conditions renseignées à l'article R. 236-22 du code de la sécurité intérieure. (Article R. 236-22 du code de la sécurité intérieure)
Critères d'inscription dans ce fichier	Toute personne d'au moins treize ans qui est susceptible selon les autorités « *de prendre part à des activités terroristes, de porter atteinte à l'intégrité du territoire ou des institutions de la République ou d'être impliquées dans des actions de violences collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives* ».
Autorité(s) compétente(s)	Direction générale de la gendarmerie nationale (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont accès à ce fichier, dans la limite du besoin d'en connaître : - Les personnels de la gendarmerie nationale individuellement désignés et spécialement habilités ; - Le ou la référente nationale et ses adjoints et adjointes instituées par l'article R. 236-15 et dans les conditions définies à l'article R. 236-15 du code de la sécurité intérieure ; - Les personnels du service à compétence nationale dénommé « service national des enquêtes administratives de sécurité », individuellement désignés et spécialement habilités par le ou la directrice générale de la police nationale ; - Les personnels du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire », individuellement désignés et spécialement habilités par le ou la directrice générale de la police nationale ; - Les personnes ayant autorité sur les services ou unités mentionnées précédemment ; - Les procureurs de la République ; - Les personnels d'un service de la police nationale ou d'une unité de la gendarmerie nationale chargés d'une mission de renseignement et les agents des services mentionnés aux articles R. 811-1 et R. 811-2 du code de la sécurité intérieure, sur autorisation expresse des commandants ou commandantes de groupement, de région ou du directeur ou la directrice générale de la police nationale ; - Les personnels de la police nationale ou les militaires de la gendarmerie nationale qui ne sont pas chargés d'une mission de renseignement sur demande expresse, précisant l'identité du demandeur, l'objet et les motifs de la communication. Les demandes sont agréées par les commandants ou commandantes de groupement, de région ou du directeur ou la directrice générale de la police nationale. (Article R. 236-26 du code de la sécurité intérieure)
Durée de conservation des données	Les données ne peuvent être conservées plus de 10 ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ou à la sûreté de l'État ayant donné lieu à un enregistrement. La durée est de 3 ans pour les personnes mineures.
Échanges de données	L'article R. 236-28 du code de la sécurité intérieure interdisant l'interconnexion des fichiers a été abrogé en 2017. - Indication de l'enregistrement ou non de la personne dans différents traitements de données à caractère personnel suivants : TAJ, N-SIS II (voir SIS II), FPR, FSPRT, FOVeS.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. - Les droits d'accès, de rectification et d'effacement **concernant les données intéressant la sûreté de l'État** s'exercent auprès de la Cnil dans les conditions prévues à l'article 118 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

	- Les droits d'information, d'accès, de rectification, d'effacement et à la limitation **concernant les autres données** s'exercent directement auprès de la direction générale de la gendarmerie nationale. Lors des enquêtes, ces droits peuvent faire l'objet de restrictions.
Remarques	Le PASP et le GIPASP sont équivalents, l'un pour la police et l'autre pour la gendarmerie. Les remarques apportées au tableau PASP sont donc les mêmes pour le GIPASP. **Une nouveauté importante :** en 2020, les fichiers peuvent aussi concerner des personnes morales ou des « groupements ». Cela pourra donc concerner des associations, collectifs etc. « *Désormais, si la police le juge nécessaire, chaque membre de l'entourage pourra avoir une fiche presque aussi complète que celle des personnes dangereuses (activités en ligne, lieux fréquentés, mode de vie, photo…)* ». En 2021, le Conseil d'État (CE) a neutralisé un des points les plus importants des deux fichiers. En effet le Gisti explique le cadrage apporté par le CE : « *la mention des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ainsi que des « données de santé révélant une dangerosité particulière » ne sauraient constituer en tant que telles des catégories de données pouvant faire l'objet d'un fichage mais que, dans l'hypothèse où des activités seraient susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État, il sera possible de ficher ces activités, même si elles font apparaître les opinions politiques, les convictions philosophiques, religieuses, l'appartenance syndicale ou des données de santé de la personne. La nuance est importante et interdit donc « un enregistrement de personnes dans le traitement fondé sur la simple appartenance syndicale.* » (Gisti, Les fichiers de police - trop peu - recadrés par le Conseil d'État, 2021) Les fichiers PASP et GIPASP ont été créés après le scandale dominant EDVIGE et EDVISRP[18]. En effet, le 7 décembre 2020, Martin Untersinger (journaliste du quotidien Le Monde) interroge Arthur Messaud, porte-parole de La Quadrature du Net, : « *Nous sommes aussi inquiets : tout ce qui avait été enlevé du fichier Edvige* [qui avait fait polémique en 2008], *à savoir le fichage des opinions politiques et religieuses, et non plus seulement des activités politiques et religieuses, a été remis.* » Les pratiques autour des fichiers GIPASP, PASP et EASP étaient déjà mises en place par les autorités compétentes sans cadre légal déclare la Cnil. En effet, elle a précisé que ces décrets tiennent « *compte de l'évolution de certaines pratiques dans l'utilisation de ce traitement, et ce faisant, les régularisent* », admettant ainsi que ces pratiques existent déjà mais *a priori* hors du cadre légal. (Cnil, Délibération n° 2020-065 du 25 juin 2020) En 2020, 67 000 personnes étaient inscrites au GIPASP.
Textes qui régissent ce fichier	- Articles R. 236-21 à R. 236-30 du code de la sécurité intérieure - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Gisti, Fichage sans limites au nom de la sécurité publique : le spectre de Big Brother en 2021, Action collective, 2020 Gisti, Les fichiers de police - trop peu - recadrés par le Conseil d'État, Action collective, 2021 Gisti, Recours contre l'extension des données enregistrées dans trois fichiers de sécurité publique, mise à jour en 2022 Januel Pierre, « L'Intérieur muscle les possibilités de fichage politique », Next, 2020 La Quadrature du net, Décrets PASP: fichage massif des militants politiques, 8 décembre 2020 Latour Xavier, « Une nouvelle extension de fichiers de police », Le Club des Juristes, 2020 Untersinger Martin, « Le gouvernement élargit par décret les possibilités de fichage », Le monde, décembre 2020 Cnil, Délibération n° 2020-065 du 25 juin 2020

[18] Le scandale des fichiers EDVIGE et EDVISRP concernait notamment la collecte de données concernant les opinions politiques et religieuses. Voir notamment Le Monde, « Fichier Edvige : les points inquiétants pour les libertés », 6 septembre 2008.

Nom du fichier	**GIPI**
Sens de l'acronyme	Gestion informatisée des procédures d'immigration
Date de création	14 février 2013
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectifs de : - Faciliter la gestion des procédures de non-admission des personnes étrangères qui ne remplissent pas les conditions d'entrée dans l'espace de libre circulation des personnes entre les États signataires de l'accord de Schengen ; - Permettre le traitement et la gestion du suivi des amendes infligées aux entreprises de transport. (Article 1 de l'arrêté du 14 février 2013) 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	L'objectif implicite du GIPI est de généraliser les procédures de surveillance dans les zones d'attente. Il permet également de faire un suivi plus efficace des amendes contre les compagnies de transport qui ont embarqué dans leurs moyens de transport des personnes qui ne remplissent pas les conditions d'entrée sur le territoire français ou l'espace Schengen. Cela permet donc l'externalisation et la privatisation des contrôles aux frontières extérieures effectuées par les compagnies de transport.
Contenu des données	- Données relatives à la personne voyageuse : 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 le cas échéant - Données relatives à la personne accompagnante : 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 : motif du maintien, motif du voyage, documents manquants, mention de la sollicitation par la personne du bénéfice du jour franc - Procédure de demande d'asile : type de documents de voyage, mention de la possession ou non de billets de voyage, date d'arrivée, date de la demande, mention de l'audition ou non par l'Ofpra (et, le cas échéant, date de cette audition), décision, date de sortie du territoire à la suite de l'octroi d'un sauf-conduit, date de fin de maintien suite à délivrance du sauf-conduit, date à laquelle le passager doit quitter le territoire, destination initiale du passager, destination indiquée sur le sauf-conduit, destination prévue pour la reconduite à la frontière si cette décision est prise par le juge, transport de sortie - Procédure de présentation de l'étranger non admis devant les juridictions compétentes : type de présentation, décision, date du recours et de l'ordonnance motif du refus de prolongation nom de la juridiction saisie et de son président, auteur de l'appel, nombre de jours accordés - Procédure de réadmission dans l'espace Schengen : type et pays de réadmission, référence, nature et pays de délivrance du document de voyage, préfecture destinataire de la demande de réadmission - Données relatives à l'hébergement de la personne non admise : compagnie aérienne concernée, aérogare, date de présentation devant l'officier de quart, modalités de prise en charge des repas et nuitées - Données relatives aux documents : type, identifiant et pays de délivrance du document, caractère authentique ou non du document, numéro du visa Schengen, mention de la possession ou non de billets de voyage, d'un document de voyage ou d'un visa par le demandeur d'asile, type et nature des faux documents présentés, nombre de documents de voyages possédés par la personne maintenue - Données relatives à l'interprète : identifiant du dossier, type de procédure, acte pour lequel l'assistance d'un interprète a été nécessaire, nom, prénom, langue parlée, société, aérogare, date de début, de fin et durée de la prestation - Données relatives aux pénalités financières infligées à l'entreprise de transport : identifiant de la procédure, libellé de la compagnie, pénalité relative à l'accompagnant, identifiant de l'accompagnant, date, numéro, motif de la pénalité, nom du rédacteur de la pénalité (Annexe de l'arrêté du 14 février 2013)
Critères d'inscription dans ce fichier	Personne s'étant vue refuser l'entrée sur le territoire Schengen aux frontières aériennes, terrestres ou maritimes en France
Autorité(s) compétente(s)	Le directeur général de la police nationale, direction nationale de la police aux frontières (ministère de l'intérieur)
Qui a accès à ce fichier ?	Ont seuls accès aux données, à raison de leurs attributions et dans la limite du besoin d'en connaître, les policiers et policières de la police nationale affectés à la direction centrale de la police aux frontières (direction centrale et services territoriaux) individuellement désignées et spécialement habilitées par leur supérieur/supérieure hiérarchique. Peuvent être destinataires* des données :

	- Le personnel de la police nationale affecté à la DNPAF et dans les services territoriaux de la PAF individuellement désigné et spécialement habilité ; - Le personnel des services de la direction générale des étrangers en France du ministère de l'intérieur ; - Le personnel de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur. (Article 4 de l'arrêté du 14 février 2013)
Durée de conservation des données	3 mois à compter de la clôture du dossier (Article 3 de l'arrêté du 14 février 2013)
Échanges de données	Aucune information concernant des échanges de données avec d'autres traitements n'est mentionnée concernant le GIPI.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès et de rectification s'exercent auprès de la direction nationale de la PAF (DNPAF) à l'adresse suivante : direction centrale de la police aux frontières, 8, rue de Penthièvre, 75008 Paris. (Article 6 de l'arrêté du 14 février 2013)
Remarques	- Le GIPI a remplacé le Fichier des non-admis (FNAD[19]). Ce dernier avait été expérimenté seulement à l'aéroport de Roissy Charles-de-Gaulle de 2007 à 2013 et était le fichier pilote du GIPI. Selon l'avis de la Cnil, le fichier GIPI aura les mêmes fonctions que le FNAD mais il sera appliqué à l'ensemble du territoire. - Le GIPI couvre les missions du FNAD, i.e « faciliter et fiabiliser [les] démarches en assurant la traçabilité de chaque dossier », et remplit de nouvelles missions notamment la gestion du suivi des amendes contre les compagnies de transport. - Le GIPI collecte les données relatives à l'hébergement de la personne non-admise, chose que le FNAD ne faisait pas. - Également, le GIPI ne garde plus les données biométriques* et les images numérisées (contrairement au FNAD) mais il garde les résultats médicaux des tests osseux des personnes se déclarant mineures et il conserve également les données de la personne accompagnante. - Ainsi, le GIPI est la conclusion du fichier expérimental FNAD et élargi à l'ensemble du territoire. (Délibération n° 2012-431 du 6 décembre 2012 de la Cnil)
Textes qui régissent ce fichier	- Articles L. 211-1 à L. 213-9, L. 221-1 à L. 224-4, L. 625-1, R. 211-1 à R. 212-11 et R. 221-1 à R. 222-4 du CESEDA - Arrêté du 14 février 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « gestion informatisée des procédures d'immigration » modifié par l'arrêté du 29 janvier 2024 modifiant diverses dispositions relatives à la police nationale - 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
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Cnil, Délibération n° 2012-431, 2012 CGLPL, *Rapport sur la visite de la zone d'attente de l'aéroport Roissy Charles-de-Gaulle*, 2013

Nom du fichier	**INEREC**
Sens de l'acronyme	Instruction et recours
Date de création	5 novembre 1990
Quelle échelle ?	Nationale
L'application* TélémOfpra	TélémOfpra est l'interface de consultation* à distance des données enregistrées dans le fichier INEREC. Cette interface peut être consultée par le personnel de l'Ofpra, des préfectures et du ministère de l'intérieur.
Objectifs officiels	INEREC est l'application* informatique relative à la gestion des dossiers des personnes demandant l'asile et de l'état civil des personnes protégées. Elle constitue la base de données d'enregistrement des demandes d'asile en France. Les objectifs du traitement INEREC sont : - Statuer sur les demandes d'asile et du statut d'apatride, notamment en organisant la convocation des personnes demandeuses à leur entretien personnel ; - Assurer la protection juridique et administrative des bénéficiaires de la protection internationale ; - Assurer le suivi du statut des bénéficiaires de la protection internationale et conduire les procédures de fin de protection ;

[19] Le fichier FNAD (fichier des non-admis) était un fichier pilote qui a donné lieu au GIPI. Il a été décidé de ne pas créer de fiche spéciale le concernant.

	- Assurer la transmission à la Cour nationale du droit d'asile des éléments du dossier des personnes ayant formé un recours devant cette juridiction et assurer la défense de l'Ofpra devant elle ; - Assurer à certains services partenaires un accès, par l'intermédiaire d'une interface distante dénommée TéIémOfpra, à certaines informations relatives à l'activité de l'Ofpra nécessaires à l'exercice de leurs missions ; - Produire des statistiques pour les besoins du pilotage de l'activité à l'Ofpra, du partage de connaissance sur l'administration de l'asile en France, de la contribution de l'établissement à l'élaboration et à la mise en œuvre des politiques publiques pertinentes et de la recherche scientifique. (Article 1 de la Décision de l'Ofpra du 22 novembre 2024)
Objectifs implicites	Cet échange d'informations entre l'Ofpra, les préfectures et le ministère de l'intérieur via TélémOfpra s'inscrit dans un contrôle grandissant et interconnecté des situations juridiques des personnes étrangères afin d'éloigner au plus vite les personnes déboutées. Dans la circulaire INTK1400684C du 11 mars 2014, le ministre de l'intérieur rappelait l'usage de TélémOfpra et donc des données contenues dans l'INEREC pour les pratiques de contrôle et d'expulsion des personnes étrangères déboutées du droit d'asile : « *Je vous rappelle par ailleurs que l'application* TélémOfpra vous permet de connaître chaque semaine les listes des dernières décisions devenues définitives de l'OFPRA ainsi que des dernières décisions notifiées par la CNDA relatives à des demandeurs d'asile déboutés domiciliés dans votre département. La réduction des délais entre, d'une part, les décisions définitives de l'OFPRA et de la CNDA et, d'autre part, le prononcé d'une OQTF, assortie d'un délai de départ, comme le prévoient les dispositions de l'article L.511-1 II du CESEDA, constitue la première étape dans le processus d'éloignement des déboutés, pour éviter que se prolonge indûment le séjour en France. L'OFPRA et la CNDA sont, pour leur part, sensibilisés à la nécessité d'une transmission aussi rapide que possible des informations qui vous sont nécessaires dans ce cadre, en application notamment de l'article R.733-32 du CESEDA. En particulier, en cas de contentieux et dans l'éventualité où le moyen tiré de la preuve de l'absence de la notification de la décision de la CNDA serait soulevé, vous demanderez à cette juridiction de vous adresser sans délai une copie de l'accusé de réception.* »
Contenu des données	Peuvent être collectés dans le traitement INEREC : - Le numéro d'identification de la procédure à l'Ofpra (numéro INEREC) - Les numéros individuel et familial d'identification du HCR - Les données relatives à l'identité - Les coordonnées postales, téléphoniques et électroniques avec date de mise à jour - La situation administrative relatives à la procédure de demande d'asile - Les données relatives aux documents (nature des documents d'identité versés au dossier, date de demande de certificats médicaux et de réponse des intéressés dans le cadre de l'instruction de leur demande et de l'exercice de la protection) - Les données relatives à la décision sur la demande, aux recours, et leurs dates - Le trigramme ou quadrigramme identifiant l'officier de protection, le rédacteur en charge de l'état civil ou le consultant juridique en charge du dossier - Les dates des demandes d'extraits de casier judiciaire (B2) et d'avis au Service national des enquêtes administratives de sécurité (SNEAS) - Les données relatives à un potentiel signalement extérieur relatif au comportement de la personne demandeuse d'asile ou bénéficiaire de la protection internationale au regard de l'ordre public - Les données relatives à une décision suite à l'engagement d'une procédure de fin de protection - La date de réception à l'Ofpra de la fiche familiale de référence - La validation de l'état civil des personnes protégées et mention d'une opposition à délivrance des actes d'état civil - La date à laquelle un livret de famille a été délivré - La date et le motif de saisine du parquet et date de réception de la réponse à l'Ofpra - La date de renonciation au statut - L'affectation et localisation du dossier Sous réserve de l'accord du président de la Cour, le traitement INEREC contient également les données relatives aux recours contentieux, par connexion au fichier informatique de gestion et de suivi de la Cour nationale du droit d'asile, dénommé Skipper-CNDA[20].

[20] Skipper est un logiciel qui est utilisé dans différentes juridictions administratives, il n'est pas centré sur le fichage des personnes étrangères. C'est pourquoi, il n'a pas été développé dans cette boîte.

	Sous réserve de l'accord, respectivement, du ministre chargé de l'immigration et de l'asile et du directeur général de l'Ofpra, le traitement INEREC contient également les données suivantes issues, par l'intermédiaire de la plateforme dénommée « Système d'information de l'administration des étrangers en France » (SI-AEF[21]), des traitements AGDREF 2 et DNA : - Numéro d'identification préfectoral pour les étrangers en France (numéro AGDREF 2) - Numéro d'identification attribué par le guichet unique à la personne demandeuse d'asile et à ses conjoint ou conjointe et enfants mineurs (numéro GU) - Numéro d'identification par l'Office français de l'immigration et de l'intégration (numéro Ofii) - Numéro d'identification au sein du système européen de comparaison des empreintes (numéro Eurodac) et existence d'un « hit » dactyloscopique - Coordonnées postales avec date de mise à jour - Situation administrative : dates d'entrée en France, d'enregistrement de la demande d'asile en préfecture, de délivrance de l'attestation de demande d'asile - Qualification de la procédure d'asile (Dublin, accélérée ou normale) - Date de délivrance de l'attestation de demande d'asile et circonstances d'entrée en France (entrée irrégulière ou régulière et pays traversés avant l'entrée en France) ; entretien de vulnérabilité conduit par l'Ofii et motif de vulnérabilité identifié Le traitement INEREC est complété par un dispositif de gestion dématérialisée des documents constitutifs des dossiers de demande de protection internationale et de conservation des fichiers numériques des enregistrements sonores des entretiens prévus à l'article R. 531-15 du CESEDA. (Article 2 de la décision du 22 novembre 2024)
Critères d'inscription dans ce fichier	Avoir déposé une demande d'asile en France
Autorité(s) compétente(s)	L'OFPRA et la CNDA
Qui a accès à ce fichier ?	Ont accès au fichier : - Le personnel de l'Ofpra. Ont accès par le biais de l'interface TélémOfpra, sur demande adressée au directeur général de l'Ofpra : - Le personnel individuellement désigné et spécialement habilité de l'administration centrale du ministère de l'intérieur (direction de l'asile, sous-direction des visas, direction des libertés publiques et des affaires juridiques) ; - Le personnel chargé de l'application de la réglementation des personnes étrangères dans les services déconcentrés de l'État, individuellement désigné et spécialement habilité par le préfet et, à Paris, par le préfet de police ; - Le personnel de l'Ofii individuellement désigné et spécialement habilité par le directeur général. Peuvent être destinataires* des données : - Le personnel de la CNDA ; - Au titre de la réglementation des personnes étrangères et de sa mise en œuvre, le personnel pouvant accéder au traitement AGDREF 2 ; - Au titre de l'accueil des personnes demandeuses d'asile, de l'intégration et de l'aide au retour, le personnel de l'Ofii individuellement désigné et spécialement habilité par le directeur général. (Articles 5, 6 et 9 de la décision du 22 novembre 2024)
Durée de conservation des données	- Pour les personnes ayant eu une décision négative à leur demande de protection internationale, la durée de conservation est de 10 ans à partir de la notification de la décision. - Les données personnelles des personnes placées sous protection de l'Ofpra sont conservées en base active durant 10 ans à compter de la date de cessation de la protection pour quelque motif que ce soit. - À l'expiration de ces délais, certaines données sélectionnées sont conservées à des fins archivistiques. (Article 10 de la décision du 22 novembre 2024)

[21] « *Le SI ANEF a pour objet la conception et/ou la refonte des applications informatiques dans les domaines de l'asile, du séjour et de l'éloignement afin de rationaliser et simplifier les démarches des usagers mais également de faciliter le travail des agents par une dématérialisation complète du dossier, de la demande à l'instruction*. » (budget.gouv). Il n'est donc pas un fichier, mais une plateforme, c'est pourquoi il n'a pas été développé dans le cadre de la présente boîte à fichiers.

Échanges de données ?	La décision du 22 novembre 2024 modifie l'arrêté du 5 novembre 1990, selon lequel le fichier ne peut faire l'objet d'aucune cession, interconnexion, mise en relation ou rapprochement* avec un autre fichier. Selon la décision du 22 novembre 2024, les données enregistrées dans le traitement INEREC peuvent être échangées : - Pour les besoins de l'exercice des missions de la CNDA, avec le traitement Skipper-CNDA ; - Pour les besoins de l'exercice des missions du ministère de l'intérieur et des préfectures, avec le traitement AGDREF 2 ; - Pour les besoins de l'exercice des missions de l'Ofii, avec le traitement DNA. Dans les cas mentionnés aux 2 et 3 ci-dessus, les échanges de données sont effectués par l'intermédiaire de la plateforme dénommée « Système d'information de l'administration des étrangers en France » (SI-AES). Selon l'article 4 de la décision, pour les besoins de la procédure contentieuse, et en application de l'article R. 532-13 du CESEDA, les dossiers numérisés des personnes demandeuses et bénéficiaires de la protection internationale ayant introduit un recours devant la CNDA, accompagnés des enregistrements sonores des entretiens prévus à l'article R. 531-15 du CESEDA, sont transmis par voie électronique au président de la Cour. Les documents de la procédure sont transmis à l'Ofpra, en sa qualité de partie au litige, par la même voie.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès et de rectification ainsi qu'à la limitation du traitement prévus aux articles 15, 16 et 18 du règlement (UE) 2016/679 du 27 avril 2016 s'exercent auprès du directeur général de l'Ofpra – à l'adresse suivante 201 rue Carnot, 94136 Fontenay-sous-Bois Cedex (Annuaire de l'administration, OFPRA, 2025)
Remarques	Des erreurs techniques entre le fichier INEREC, l'interface TélémOfpra et la plateforme ANEF peuvent engendrer des impossibilités d'obtenir un titre de séjour du fait des démarches dématérialisées. (Pradines Dorothée, Rapporteure publique, Conclusions n° 497272, *Ofpra c/ Mme M*, Conseil d'État, séance du 8 janvier 2025)
Textes qui régissent ce fichier	- Articles R. 530-1 à R. 532-72 du CESEDA - 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 - Décision du directeur général de l'OFPRA du 22 novembre 2024 relative au traitement automatisé de données à caractère personnel dénommé Inerec et à son interface de consultation* à distance dénommée *TélémOfpra* - Délibération n° 90-88 du 10 juillet 1990 de la Cnil relative à un traitement automatisé d'informations nominatives concernant la gestion des formalités administratives relevant de l'OFPRA - 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 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » La Cimade, « Abécédaire des migrations » Lochak Danièle, « Des fichiers pour gérer, contrôler et surveiller les étrangers », *Plein droit*, n° 71, 2006 Ministère de l'intérieur, Circulaire INTK1400684C, 11 mars 2014 Pradines Dorothée, Rapporteure publique, Conclusions n°497272, *Ofpra c/ Mme M*, Conseil d'État, séance du 8 janvier 2025

Nom du fichier	**LOGICRA**
Sens de l'acronyme	Logiciel* de gestion individualisée des centres de rétention administrative
Date de création	Mars 2018
Quelle échelle ?	Nationale
Objectifs officiels	Gestion quotidienne et opérationnelle de la rétention administrative des personnes étrangères et de ses différentes étapes et production de données statistiques
Objectif implicite	Contrôler et surveiller les personnes étrangères dans les centres de rétention et rendre effectif leur éloignement. Participe à faciliter l'éloignement le refoulement des personnes.
Contenu des données	Données relatives à la personne étrangère placée en rétention administrative : - Nom(s), prénom(s), alias éventuels ; Date et lieu de naissance, nationalité ; Sexe - Situation familiale, nom(s), prénom(s) et âge des enfants mineurs accompagnants

	- Photographie d'identité - Type et validité du document d'identité éventuel - Numéro de l'application de gestion des dossiers des ressortissants étrangers en France correspondant au dossier de l'étranger placé en rétention - Le cas échéant, qualité de sortant de prison - Signature Données relatives à la procédure administrative de placement en rétention administrative : - Date et heure du prononcé et de la notification de l'arrêté préfectoral de placement en rétention et, le cas échéant, des décisions de prolongation - Lieu de placement en rétention, date et heure d'admission au centre de rétention administrative, date et heure d'un transfert d'un lieu de rétention administrative à un autre lieu de rétention et motif - Préfecture en charge de l'exécution de la mesure de placement en centre de rétention administrative - Service interpellateur ou réalisant le transfert : transfert éventuel depuis un autre centre de rétention administrative ou depuis un établissement pénitentiaire - Droits de la personne liés au placement en rétention (date et heure de la notification des droits, référence du procès-verbal de notification) - Agente ou agent chargé de la mesure d'admission en centre de rétention administrative : nom, prénom, grade, numéro d'identification, signature - Conditions particulières d'accueil, secteur d'hébergement, affectation d'une chambre et d'un lit - Origine, nature et date de la mesure d'éloignement, date de sa notification, interdiction de retour - Bagages placés en consigne : numéro de registre et de consigne, détail et état des bagages, date de restitution des bagages - Biens placés au coffre : numéro de registre et de coffre, liste des objets de valeur et des objets écartés, date de dépôt et de restitution - Objets laissés à la disposition de la personne retenue - Mouvements d'argent : numéro de registre, détail du numéraire, date et heure de dépôt et de retrait des fonds - Compte rendu des incidents au centre de rétention (date, heure, circonstances) : mise à l'écart, dates de début et de fin de la mise à l'écart et avis de cette mesure aux autorités judiciaires et administratives compétentes, nom, prénom, grade et numéro d'identification de l'agent ayant décidé la mise à l'écart, date et heures d'une demande d'examen médical et, le cas échéant, date et heure de l'examen médical et des mesures prescrites nécessitant l'intervention du personnel du centre de rétention administrative - Hospitalisation éventuelle : date et heure d'admission, coordonnées de l'établissement hospitalier, date et heure de sortie - Existence d'une procédure « étranger malade » : date de saisine de l'agence régionale de santé (ARS), avis de l'ARS, décision préfectorale - Nom, prénom et signature de l'interprète - Nom, prénom, grade et signature du personnel du centre de rétention administrative Données relatives aux procédures juridictionnelles mises en œuvre au cours de la rétention : - Contentieux administratif : type de recours, juridiction saisie, date et heure de l'audience, décision, appel - Contentieux judiciaire : présentation devant le ou la juge judiciaire et saisine par la personne retenue, date de présentation, décision, appel, date d'audience de la cour d'appel, résultat, motif d'annulation - Demande d'asile : date et heure du dépôt de la demande, modalité d'instruction, décision de l'Ofpra et date de celle-ci, recours auprès de la CNDA Données relatives à la fin de la rétention et à l'éloignement : - Demande de laissez-passer consulaire, consulat saisi, date de la demande d'identification ou de présentation consulaire, type de présentation, motif de non-présentation, date de l'entretien, moyen de transport utilisé, résultat de l'entretien, délivrance du laissez-passer consulaire, date de délivrance, date et fin de validité du laissez-passer consulaire - Réservation du moyen de transport national et international : date prévisionnelle de départ, moyen de transport utilisé, pays de destination, demande de routing, escorte - Fin de la rétention : date et motif de la fin de rétention (Article 2 et Annexe de l'arrêté du 6 mars 2018)
Critères d'inscription dans ce fichier	Personne placée en rétention administrative

Autorité(s) compétente(s)	Le directeur général de la police nationale (Article 1 de l'arrêté du 6 mars 2018)
Qui a accès à ce fichier ?	Ont accès à tout ou en partie : - Le personnel de la police nationale ; - Le personnel des préfectures et de la préfecture de police ; - Le personnel du bureau chargé de la rétention et de l'éloignement à la direction générale des étrangers en France. Ces personnels sont individuellement désignés et habilités par l'autorité hiérarchique dont ils relèvent. (Article 3 de l'arrêté du 6 mars 2018)
Durée de conservation des données	2 ans à compter de la sortie définitive du centre de rétention administrative. Pour les personnes dont la mesure d'éloignement a été annulée, abrogée ou retirée, les données à caractère personnel doivent être effacées du traitement LOGICRA par le centre de rétention dès réception de la décision. (Article 4 de l'arrêté du 6 mars 2018)
Échanges de données ?	Aucune information concernant des échanges de données avec d'autres traitements n'est mentionnée concernant LOGICRA.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès et de rectification des données s'exercent auprès de la direction centrale de la police aux frontières et, en ce qui concerne les personnes ayant été ou étant retenue dans un centre de rétention administrative de Paris, ces droits s'exercent auprès de la préfecture de police. (Article 6 de l'arrêté du 6 mars 2018)
Remarques	La mise en œuvre du traitement LOGICRA s'est accompagnée de la création d'un registre « *dans tous les lieux recevant des personnes placées ou maintenues* » mentionnant l'état civil et les conditions du placement ou du maintien pour chaque personne. La création de ce registre, autorisée par l'arrêté du 6 mars 2018, était prévue à l'article L. 553-1 du CESEDA en vigueur entre le 18 juin 2011 et le 1er mai 2021. Cet article a été abrogé par l'Ordonnance n° 2020-1733 du 16 décembre 2020. L'arrêté du 6 mars 2018 portant autorisation de la mise en œuvre du traitement LOGICRA a été adopté avant la loi n° 2024-42 du 26 janvier 2024 pour « *contrôler l'immigration, améliorer l'intégration* », interdisant le placement en rétention administrative des personnes mineures, même accompagnées d'un parent. Par conséquent, les données relatives au(x) mineur(es) accompagnant une personne placée en rétention ne peuvent plus être enregistrées dans le traitement LOGICRA. Dans son avis du 7 décembre 2017 sur le projet d'arrêté portant autorisation du traitement LOGICRA, la Cnil souligne la similarité des objectifs des traitements LOGICRA et AGDREF 2 qui concernent tous deux la gestion des procédures relatives à l'éloignement des personnes étrangères. À cet égard, la Cnil remarque que certaines données, telles que celles relatives aux bagages placés en consigne, sont collectées dans les deux traitements, sans que cela soit justifié. La Cnil reconnaît toutefois la nuance entre les deux traitements : l'AGDREF 2 « *a pour objet la gestion administrative globale de l'ensemble des ressortissants étrangers, et non pas uniquement de ceux qui sont en situation irrégulière, tandis que le traitement LOGICRA n'a qu'une vocation opérationnelle, centrée sur la gestion quotidienne, par les CRA, des seules personnes faisant l'objet d'un placement en rétention administrative* ». Lors de la réunion annuelle sur le fonctionnement des zones d'attente de 2018, la direction centrale de la police aux frontières a annoncé que des travaux étaient en cours afin de mettre en place un traitement similaire à LOGICRA pour les zones d'attente, appelé « LOGIZA ». L'objectif de ce traitement serait de regrouper le même type de données et de pouvoir produire des statistiques sur l'ensemble des zones d'attente de France. Or, c'est la seule fois qu'il a été fait mention d'un tel outil, et aucune information relative aux travaux de mise en place de LOGIZA n'est disponible à l'heure de la publication de ce document.
Textes qui régissent ce fichier	- Arrêté du 6 mars 2018 portant autorisation du registre de rétention prévu à l'article L. 553-1 du CESEDA et d'un traitement automatisé de données à caractère personnel dénommé « logiciel* de gestion individualisée des centres de rétention administrative » (LOGICRA) - Délibération n° 2017-323 du 7 décembre 2017 de la Cnil (demande d'avis n° 1936397) - 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 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Compte-rendu de la réunion annuelle sur le fonctionnement des zones d'attente, 2018

Nom du fichier	**OSCAR**
Sens de l'acronyme	Outil de statistique et de contrôle de l'aide au retour
Date de création	26 octobre 2009
Quelle échelle ?	Nationale
Objectifs officiels	Ce traitement a pour finalité de : - 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'Ofii ; - Établir des statistiques relatives à ces procédures et à leur exécution. (Article R. 142-33 du CESEDA)
Objectif implicite	Entraver la liberté de circulation de Roms roumains ou bulgares ayant déjà fait l'objet d'une aide au retour. En effet, bien que le fichier OSCAR vise l'ensemble des étrangers susceptibles de bénéficier d'une aide au retour, plusieurs associations (Gisti, Iris, LDH) 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. Selon Meryem Marzouki, « *Les statistiques prévues dans le fichier OSCAR permettent surtout d'appréhender l'activité des services concernés et de mesurer l'activité de leurs responsables personnes physiques. On passerait alors, de manière subreptice, d'un objectif légitime et nécessaire d'information des politiques publiques à un objectif de contrôle, d'évaluation voire de sanction du personnel administratif en charge de l'exécution de ces politiques. [...]* *De plus, comme le soulignent les associations dans leur recours contre le décret OSCAR, la finalité statistique relève d'un objectif gestionnaire sévèrement encadré par les textes législatifs et réglementaires, notamment afin d'interdire la possibilité d'identifier les personnes à partir des résultats statistiques. Étant donné que les articles de loi visés par le décret ne peuvent servir de fondement à un traitement à finalité statistique, il y a donc là encore une extension illégale de la finalité.* »
Contenu des données	Données relatives aux informations d'identification de l'étranger bénéficiaire de l'aide au retour : - Noms et prénoms, sexe, situation maritale déclarée, date et lieu de naissance, nationalité, coordonnées du bénéficiaire en France et dans le pays de retour, photographie d'identité - Date d'entrée en France - Numéro national d'identification mentionné au 2° de l'article D. 611-2 du CESEDA - Numéro, date et lieu de délivrance du passeport ou laissez-passer - Motifs de la demande : situation de dénuement, volonté de départ - Nombre de personnes concernées par la mesure, liens unissant les bénéficiaires - Mesure d'éloignement, date et nature Gestion administrative et comptable du dossier : - Numéro de dossier ; Date de la décision de l'Ofii ; Numéro de l'ordre de paiement ; Nature et montant de l'aide accordée ; Dates et montants des versements effectués ou à effectuer ; Autres secours dont aide exceptionnelle d'acheminement Organisation du voyage : - Hébergement avant départ - Moyens de transport - Date et lieu du départ du territoire français - Pays et ville de destination (Annexe 5 du CESEDA) - Les images numérisées des empreintes des dix doigts du bénéficiaire et de ses enfants mineurs d'au moins 12 ans 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 personnes étrangères concernées, sauf en cas de réquisition judiciaire. Il ne comporte pas non plus de dispositif de reconnaissance faciale à partir de la photographie. (Article R. 142-35 du CESEDA)

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. (Article R142-34 du CESEDA)
Autorité(s) compétente(s)	Ofii
Qui a accès à ce fichier ?	Ont accès : - Le personnel de l'Ofii chargé de la mise en œuvre du dispositif d'aide au retour est le seul à avoir un accès direct*. (Article R. 142-36 du CESEDA) Peuvent être destinataires* des données, à l'exclusion des données biométriques* : - Le personnel préfectoral compétent pour l'application de la réglementation relative aux étrangers, afin d'assurer le suivi administratif des procédures d'attribution des aides au retour ; - Le personnel des ambassades et des consulats français à l'étranger afin de pouvoir assurer le suivi de la procédure après le départ en France ; - Le personnel 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. (Article R. 142-37 du CESEDA)
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 5 ans à compter de la date de la décision de l'OFII. - Lorsque l'aide au retour volontaire est refusée ou que l'intéressé y renonce, les données sont effacées sans délai. Les personnes intéressées sont informées par écrit dans une langue qu'elles comprennent des conditions de conservation des données les concernant, de leur droit d'accès à ces données et des destinataires* de ces données. (Article R. 142-38 du CESEDA)
Échanges de données	Aucune précision législative sur une interconnexion ou sur l'interdiction de celle-ci.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. (Article R. 142-40 du CESEDA) Les personnes doivent être informées par écrit et dans une langue qu'ils et elles comprennent des conditions de conservation des données, de leur droit d'accès à ces données et des destinataires* de ces données. Cette information est effectuée par une mention sur le formulaire de demande d'aide au retour et sur le site internet de l'OFII, ainsi que par voie d'affichage dans les locaux de l'office. (Cnil, le fichier OSCAR, 2010) Les droits d'accès et de rectification aux données qui les concernent, s'exercent directement auprès du directeur général de l'Ofii : OFII, 44 rue Bargue - 75732 Paris Cedex 15 Tél. : 01 53 69 53 70 Le délais moyen prévu pour la communication des informations demandées est d'un mois. (Article R. 142-39 du CESEDA)
Remarques	Meyrem Marzouki rappelle que « *le décret Oscar ne précise pas, contrairement au décret Eloi, que les données enregistrées dans ce fichier ne peuvent faire l'objet de rapprochement* avec aucun autre fichier. Des interconnexions avec d'autres fichiers sont donc prévisibles, en particulier avec les fichiers des caisses d'allocations familiales. Au demeurant, comme de nombreux autres fichiers, Oscar existait avant même sa création officielle, et une saisine de la Cnil par le Collectif Romeurope en avril 2009 s'inquiétait déjà de « plusieurs indices qui laissent supposer que des informations contenues dans le fichier Oscar sont transmises à diverses administrations* » (voir Saisine Cnil par Romeurope, 2009). » Enfin, elle souligne que « *Pour ce qui est d'Oscar, la Cnil prend également acte de la finalité statistique du fichier dans son avis sur le projet de décret, et demande que des précisions quant à l'anonymat des statistiques et au but poursuivi par leur élaboration. Le gouvernement n'en a fait aucun cas, puisque le décret publié n'intègre aucune de ces précisions* ». (Meryem Marzouki, « Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire ? », 2010) Le collectif Romeurope revendique notamment « l'abrogation du dispositif de fichage biométrique des bénéficiaires de l'aide au retour humanitaire prévu par la loi du 20 novembre 2007 et le décret n° 2009-1310 du 26 octobre 2009, avec dans l'attente le contrôle de la stricte confidentialité des informations conservées dans le fichier "OSCAR" et l'absence de transmission aux administrations sociales. »
Textes qui régissent ce fichier	- Articles R. 142-33 à R. 142-40 du CESEDA - 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 - Délibération n° 2009-468 du 16 juillet 2009 de la Cnil 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 CESEDA

	- 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
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Cnil, « OSCAR : Outil de Statistique et de Contrôle de l'Aide au Retour », 2010 LDH, « Oscar ou le déni de citoyenneté européenne des Roms », 2010 Marzouki Meryem, « Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire ? », Mouvements.info, 2010 Ofii, *Rapport annuel 2023*, 2023, p. 55 à 59 (statistiques sur l'aide au retour)

Nom du fichier	**PASP**
Sens de l'acronyme	Prévention des atteintes à la sécurité publique
Date de création	2009
Quelle échelle ?	Nationale
Objectifs officiels	Le PASP a pour finalité de : - Recueillir, conserver et analyser les informations qui concernent des personnes physiques ou morales ainsi que des groupements dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'État ; - Recueillir, conserver et analyser les informations qui concernent les personnes susceptibles de prendre part à des activités terroristes, de porter atteinte à l'intégrité du territoire ou des institutions de la République ou d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives. Les données intéressant la sûreté de l'État sont celles qui révèlent des activités susceptibles de porter atteinte aux intérêts fondamentaux de la Nation ou de constituer une menace terroriste portant atteinte à ces mêmes intérêts. Ces données, de façon isolée ou groupée, font l'objet d'une identification dans le traitement. (Article R. 236-11 du code de la sécurité intérieure)
Objectifs implicites	Ce traitement de données* permet le fichage massif de militantes et militants politiques, de leur entourage (notamment de leurs enfants mineurs), de leur santé ou de leurs activités sur les réseaux sociaux.
Contenu des données	Données concernant la personne physique pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État : - Éléments d'identification : Noms, prénoms, alias, date et lieu de naissance, nationalité, signes physiques particuliers et objectifs, photographies, documents d'identité (type, numéro, validité, autorité et lieu de délivrance), origine géographique (lieux de résidence et zones d'activité) - Coordonnées : Numéros de téléphone, adresses postales et électroniques, identifiants utilisés (pseudonymes, sites ou réseaux concernés, autres identifiants techniques), à l'exclusion des mots de passe, adresses et lieux fréquentés - Situation : Situation familiale, formation et compétences, profession et emplois occupés, moyens de déplacement (moyens utilisés, immatriculation des véhicules, permis de conduire), situation au regard de la réglementation de l'entrée et du séjour en France, éléments patrimoniaux Motifs de l'enregistrement : - Activités susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État : Activités publiques ou au sein de groupements ou de personnes morales, comportement et habitudes de vie, déplacements, activités sur les réseaux sociaux, pratiques sportives, pratique et comportement religieux - Facteurs de dangerosité : Lien avec des groupes extrémistes, éléments ou signes de radicalisation, suivi pour radicalisation, données relatives au troubles psychologiques ou psychiatriques obtenues conformément aux dispositions législatives et réglementaires en vigueur ; armes et titres afférents ; détention d'animaux dangereux ; agissements susceptibles de recevoir une qualification pénale ; antécédents judiciaires (nature des faits et date) ; fiches de recherche ; suites judiciaires ; mesures d'incarcération (lieu, durée et modalités) ; accès à des zones ou des informations sensibles ; - Facteurs de fragilité : Facteurs familiaux, sociaux et économiques ; régime de protection ; faits dont la personne a été victime ; comportement auto-agressif ; addictions ; mesures administratives ou judiciaires restrictives de droits, décidées ou proposées ; - Indication de l'enregistrement ou non de la personne dans les traitements de données à caractère personnel suivants : TAJ, N- SIS (voir SIS II), FPR, FSPRT, FOVeS. Données concernant les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne pouvant porter atteinte à la sécurité publique ou la sûreté de l'État, notamment ses parents et ses enfants, dans la stricte mesure où ces données sont nécessaires pour son suivi et dans la limite des catégories mentionnées aux 1°, 2°, 3° et 5° à l'exception du c du I

	Données concernant les victimes des agissements de la personne physique pouvant porter atteinte à la sécurité publique ou la sûreté de l'État, dans la stricte mesure où ces données sont nécessaires à la protection des intérêts de la victime et à la prévention de la réitération de faits par la personne concernée et dans la limite des catégories mentionnées aux 1°, 2°, 3°, 5° à l'exception du c du I et au c du 7° du I Données concernant les personnes physiques entretenant ou ayant entretenu des relations directes et non fortuites avec la personne morale ou le groupement pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État, ou victimes des agissements de ces personnes morales et groupements, dans la stricte mesure où ces données sont nécessaires à leur suivi et dans la limite des catégories mentionnées aux 1°, 2°, 3°, 5° à l'exception du c du I, et, concernant les victimes, au c du 7° du I (Article R. 236-21 du code de la sécurité intérieure)
Critères d'inscription dans ce fichier	Personne d'au moins 13 ans pouvant porter atteinte à la sécurité publique ou à la sûreté de l'État
Autorité(s) compétente(s)	La direction générale de la gendarmerie nationale (ministère de l'intérieur)
Qui a accès à ce fichier ?	Dans la limite du besoin d'en connaître, y compris pour des enquêtes administratives sous conditions, sont autorisés à accéder aux données enregistrées dans le traitement : - Les personnels de la gendarmerie nationale individuellement désignés et spécialement habilités ; - Le ou la référente nationale et ses adjoints ou adjointes instituées par l'article et avec les conditions définies par l'article R. 236-15 et R.236-21 du code de la sécurité intérieure. Dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives, peuvent être destinataires* des données mentionnées aux articles R. 236-22 et R. 236-23 : - Les membres du personnel du service à compétence nationale dénommé « service national des enquêtes administratives de sécurité », individuellement désigné et spécialement habilité par la direction générale de la police nationale ; - Les membres du personnel du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire », individuellement désignés et spécialement habilités par le directeur général de la gendarmerie nationale. Dans la limite du besoin d'en connaître, peuvent être destinataires* des données mentionnées aux articles R. 236-22 et R. 236-23 du code de la sécurité intérieure : - Les personnes ayant autorité sur les services ou unités mentionnées aux deux premiers points ; - Les procureurs de la République ; - Le personnel d'un service de la police nationale ou d'une unité de la gendarmerie nationale chargés d'une mission de renseignement et les agents des services mentionnés aux articles R. 811-1 et R. 811-2 du code de la sécurité intérieure, sur autorisation expresse du commandement de groupement, de région ou de la direction générale de la gendarmerie nationale ; - Le personnel de la police nationale ou les militaires de la gendarmerie nationale qui ne sont pas chargés d'une mission de renseignement sur demande expresse, précisant l'identité du demandeur, l'objet et les motifs de la communication. Les demandes sont agréées par le commandement de groupement, de région ou de la direction générale de la gendarmerie nationale.
Durée de conservation des données	Les données ne peuvent être conservées plus de 10 ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ou à la sûreté de l'État ayant donné lieu à un enregistrement. Si la personne a entre 13 et 18 ans alors la conservation de données est de maximum 3 ans. (Article R. 236-25 du CESEDA)
Échanges de données	L'article R. 236-28 assurant l'interdiction de l'interconnexion du ficher avec d'autres fichiers a été abrogé par décret en 2017. Dans le texte régissant le fichier PASP : - Indication de l'enregistrement ou non de la personne dans les traitements de données à caractère personnel suivants : TAJ, SIS II, FOVeS, FSPRT. (Article R. 236-21 du code de la sécurité intérieure) Selon la Quadrature du net : « *les nouveaux décrets prévoient que les notes individuelles mentionneront si la personne concernée est aussi fichée dans l'un des 5 autres grands fichiers de police (GIPASP, EASP, TAJ, N-SIS [voir SIS II], fichier des personnes recherchées [FPR], FSPRT, fichiers des objets et véhicules volés ou signalés [FOVeS]).* » De plus, la notion de « sûreté de l'Etat » permet d'avoir accès aux photographies contenues dans le fichier TES, destiné à centraliser les photos de tout détenteur de passeport et de carte d'identité. Une fois obtenues, les photographies pourront être ajoutées au PASP ou au GIPASP. Rapport du référent national « mineurs » d'octobre 2024 : « *Depuis la fin 2020, l'utilisateur habilité se soumet à une authentification « forte » par l'insertion de sa carte professionnelle dans un lecteur de carte, puis par un mot de passe. Chaque action individuelle effectuée dans le traitement PASP est enregistrée pendant 3 ans.* »

Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès, de rectification et d'effacement concernant les données intéressant la sûreté de l'État s'exercent auprès de la Cnil dans les conditions prévues à l'article 110 de la loi n° 78-17 du 6 janvier 1978. Les droits d'information, d'accès, de rectification, d'effacement et à la limitation concernant les autres données s'exercent directement auprès de la direction générale de la gendarmerie nationale : formulaire de contact. Afin d'éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ou d'éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, de porter atteinte à la sécurité publique ou la sécurité nationale, les droits mentionnés aux articles 104 à 106 de la loi n° 78-17 du 6 janvier 1978, peuvent faire l'objet de restrictions en application des II et III de l'article 107 de la loi n° 78-17 du 6 janvier 1978. La personne concernée par ces restrictions exerce ses droits auprès de la Cnil dans les conditions prévues à l'article 108 de la même loi. (Article R. 236-29 du code de la sécurité intérieure)
Remarques	Selon la Quadrature du net « Si, via la loi sécurité globale, tous les manifestants pourront être filmés en manifestation et que, via le fichier TAJ, une grande partie d'entre eux pourra être identifiée par reconnaissance faciale, le PASP et le GIPASP leur a déjà préparé une fiche complète où centraliser toutes les informations les concernant, sans que cette surveillance ne soit autorisée ni même contrôlée par un juge. » Début novembre 2020, 60 686 personnes étaient inscrites au PASP, chiffre obtenu auprès du ministère de l'intérieur par le journal l'usine digitale. Rapport du référent national « mineurs » d'octobre 2024: « Dans son rapport à la Cnil pour 2022, le SCRT [gestionnaire principal du traitement PASP] a mentionné que le traitement PASP comportait au 31 décembre 2022 60 861 individus, dont 2 361 mineurs (3,88%) dont 850 devenus majeurs au cours de l'année. » Nouveauté importante : les fichiers peuvent aussi concerner des personnes morales ou des « groupements ». Cela pourra donc concerner des associations, collectifs etc. « Désormais, si la police le juge nécessaire, chaque membre de l'entourage pourra avoir une fiche presque aussi complète que celle des personnes dangereuses (activités en ligne, lieux fréquentés, mode de vie, photo…). » En 2021, le Conseil d'État a neutralisé un des points les plus importants des deux fichiers. En effet le Gisti explique le cadrage apporté par la CE : « *la mention des opinions politiques, des convictions philosophiques, religieuses ou une appartenance syndicale ainsi que des « données de santé révélant une dangerosité particulière » ne sauraient constituer en tant que telles des catégories de données pouvant faire l'objet d'un fichage mais que, dans l'hypothèse où des activités seraient susceptibles de porter atteinte à la sécurité publique ou à la sûreté de l'État, il sera possible de ficher ces activités, même si elles font apparaître les opinions politiques, les convictions philosophiques, religieuses, l'appartenance syndicale ou des données de santé de la personne. La nuance est importante et interdit donc « un enregistrement de personnes dans le traitement fondé sur la simple appartenance syndicale »* ». (Gisti, Les fichiers de police - trop peu - recadrés par le Conseil d'État, 2021) Le PASP a été créé après le scandale dominant EDVIGE et EDVISRP[22]. En effet le 7 décembre 2020, Martin Untersinger (journaliste à Le Monde) interroge Arthur Messaud, porte-parole de La Quadrature du Net, : « *Nous sommes aussi inquiets : tout ce qui avait été enlevé du fichier Edvige* [qui avait fait polémique en 2008], *à savoir le fichage des opinions politiques et religieuses, et non plus seulement des activités politiques et religieuses, a été remis.* » Les pratiques autour des fichiers GIPASP, PASP et EASP étaient déjà mises en place par les autorités compétentes sans cadre légal déclare la Cnil. En effet, elle a précisé que ces décrets tiennent « *compte de l'évolution de certaines pratiques dans l'utilisation de ce traitement, et ce faisant, les régularisent* », admettant ainsi que ces pratiques existent déjà mais *a priori* hors du cadre légal.
Textes qui régissent ce fichier	- Articles R. 236-21 à R. 236-30 du code de la sécurité intérieure - Délibération n° 2020-064 du 25 juin 2020 de la Cnil portant avis sur un projet de décret modifiant les dispositions du code de la sécurité intérieure relatives au traitement de données* à caractère personnel dénommé « Prévention des atteintes à la sécurité publique » (demande d'avis n° 19013316) - 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
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Besse Raphaëlle et Martin Untersinger, Opinions politiques et syndicales, religion, santé : l'élargissement de trois fichiers policiers provoque l'inquiétude, 2020

[22] Le scandale des fichiers EDVIGE et EDVISRP concernait notamment la collecte de données concernant les opinions politiques et religieuses. Pour plus d'informations, voir notamment Le Monde, « Fichier Edvige : les points inquiétants pour les libertés », 6 septembre 2008.

	La Quadrature du net, Décrets PASP: Fichage massif des militants politiques, *Ritimo,* 2020 Ministère de l'intérieur, Rapport du référent national « mineurs » d'octobre 2024, 2024 Januel Pierre, L'Intérieur muscle les possibilités de fichage politique, *Next,* 2020 Untersinger Martin, Le gouvernement élargit par décret les possibilités de fichage, *Le Monde,* 2020 Untermaier Cécile, Question écrite n° 35323 : Publication des décrets PASP, GIPASP et EASP relatifs aux données personnelles, Assemblée nationale, publication au Journal officiel en 2020 Vitard Alice, Le recours contre le fichage policier des données personnelles est rejeté par la justice, *Usine digitale*, 2021

Nom du fichier	**SCA ou ADOC**
Sens de l'acronyme	Système de contrôle automatisé ou accès au dossier des contraventions
Date de création	13 octobre 2004
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectif de : - Constater, au moyen d'appareils de contrôle automatique homologués, les infractions prévues à l'article R. 130-11 du code de la route ; - Procéder à l'enregistrement et à la conservation des données recueillies par l'agent verbalisateur au moyen d'appareils électroniques à l'occasion de la constatation des infractions faisant l'objet d'une procédure d'amende forfaitaire ; - Gérer les opérations relatives à l'identification des conducteurs de véhicule, auteurs d'infractions visées au 1° et au 2° ; - Gérer les opérations nécessaires au traitement des infractions visées au 1° et au 2° en vue de la notification des avis de contravention et des avis d'amende forfaitaire délictuelle ; - Gérer les réponses des personnes destinataires* d'un avis de contravention ou d'un avis d'amende forfaitaire délictuelle qui leur est notifié ; - Faciliter la gestion du paiement des consignations, le recouvrement des amendes et le remboursement des consignations par les services compétents ; - Faciliter l'établissement des retraits de points par le service chargé de la gestion du système national des permis de conduire ; - Assurer la transmission des dossiers relatifs aux infractions visées au 1° et au 2° aux tribunaux et autorités judiciaires compétents ; - Gérer le parc des appareils électroniques d'enregistrement. (Article 1 de l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé)
Objectifs implicites	Le fichier SCA ou ADOC a été créé en 2004 avec l'utilisation des radars automatiques en France. La Quadrature du Net a déposé un recours devant le Conseil d'État en novembre 2020 car le fichier a été élargi à des fins de contrôles qui ne se limitent plus aux délits routiers. En effet, la Quadrature du Net écrit : « *en avril 2020 pendant le confinement, le gouvernement a détourné ce fichier pour y inscrire des informations relatives au non-respect du confinement. La police et la gendarmerie l'ont ainsi utilisé pour repérer les récidivistes, afin tout simplement, de les mettre en prison. [ainsi] toute infraction réprimée par une amende forfaitaire sera inscrite dans ce fichier, et cela pour une durée de 5 ans (pour les contraventions) à 10 ans (pour les délits)* ». Le site Lexbase a expliqué comment le fichier SCA (ou appelé également ADOC) a été élargi : « *L'arrêté du 14 avril 2020, publié au Journal officiel du 16 avril 2020, modifie l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé en remplaçant la mention « contraventions et délits relatifs à la circulation routière » par les mots : « infractions faisant l'objet d'une procédure d'amende forfaitaire », ce qui permet d'intégrer officiellement dans ce fichier de police les infractions liées aux mesures de confinement* ». Ainsi, le fichier SCA ou ADOC a largement été élargi depuis le confinement, permettant un fichage massif de la société française. Le fichier n'est plus limité aux infractions routières, toute personne commettant une infraction réprimée par une amende de plus de 135 euros est inscrite dans le fichier.
Contenu des données	Sont enregistrées dans le système contrôle automatisé les catégories de données suivantes : - Pour les i**nfractions relatives à la circulation routière** : numéro d'identification unique de l'infraction ; clichés concernant le véhicule et ses passagers relatifs aux infractions visées à l'article 1er (1°) ; données relatives à l'infraction : nature de l'infraction, lieu, date et heure, voie contrôlée, moyens de constatation, identifiant et nom, corps et unité ou service d'affectation des agents verbalisateurs ; identification du véhicule : catégorie et numéro d'immatriculation du véhicule ayant servi à commettre l'infraction ; identification du titulaire du certificat d'immatriculation du véhicule ayant servi à commettre l'infraction : état civil : nom, nom d'usage, prénoms, date et lieu de naissance, nationalité, adresses postale et électronique ; nom ou raison sociale de la personne morale, numéro SIREN, adresse du siège social ; identification du conducteur du véhicule ayant servi à commettre l'infraction : état civil : nom, nom d'usage, prénoms, date et lieu de naissance, nationalité, adresses postale et électronique, filiation lorsque ce renseignement est nécessaire à l'identification de l'intéressé, notamment en cas d'homonymes, ou lorsque l'intéressé est né à l'étranger ; catégorie et numéro de permis de conduire du conducteur du véhicule ayant servi à commettre l'infraction ; montant de l'amende, nature ; informations relatives au paiement des amendes et des consignations

	par les débiteurs ; informations relatives au retrait de points correspondant à l'infraction ; informations relatives aux requêtes en exonération et aux réclamations présentées par les intéressés en application des articles 495-18 à 495-20 et 529-10 du code de procédure pénale ; statut des décisions rendues par les juridictions compétentes aux fins de permettre le remboursement de la consignation par les services compétents et de clôturer le dossier d'infraction - Pour les autres infractions faisant l'objet d'une procédure d'**amende forfaitaire** : numéro d'identification unique de l'infraction ; données relatives à l'infraction : nature de l'infraction, lieu, date et heure, identifiant et nom, corps et unité ou service d'affectation des agents verbalisateurs ; identification de la personne physique ou morale auteur de l'infraction : état civil : nom, nom d'usage, prénoms, date et lieu de naissance, nationalité, adresses postale et électronique, filiation lorsque ce renseignement est nécessaire à l'identification de l'intéressé, notamment en cas d'homonymes, ou lorsque l'intéressé est né à l'étranger ; nom ou raison sociale de la personne morale, numéro SIREN, adresse du siège social ; montant de l'amende, nature ; informations relatives au paiement des amendes et des consignations par les débiteurs ; informations relatives aux requêtes en exonération et aux réclamations présentées par les intéressés en application des articles 495-18 à 495-20 du code de procédure pénale En tant que de besoin, le système contrôle automatisé peut également **enregistrer des données communiquées par des États** qui présentent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. (Article 3 de l'arrêté du 13 octobre 2004) Les opérations de collecte, de modification, de consultation, de communication et d'effacement des données à caractère personnel et informations font l'objet d'un enregistrement comprenant l'identifiant de l'auteur, la date, l'heure et la nature de l'opération. Ces informations sont conservées pendant 1 an. (Article 7-1 de l'arrêté du 13 octobre 2004)
Critères d'inscription dans ce fichier	Personne ayant commis une infraction relative à la circulation routière ou infractions faisant l'objet d'une procédure d'amende forfaitaire
Autorité(s) compétente(s)	Sous le contrôle et l'autorité du ministre de l'intérieur, de la sécurité intérieure et des libertés locales (Article 1 de l'arrêté du 13 octobre 2004)
Qui a accès à ce fichier ?	Pour les infractions relatives à la circulation routière : Ont accès à tout ou partie des données à caractère personnel et informations mentionnées à l'article 3, à raison de leurs attributions et dans la limite du besoin d'en connaître : - Le personnel du Centre national de traitement et de l'Agence nationale de traitement automatisé des infractions pour l'exercice de leur compétence ; - Les autorités judiciaires ; - Le personnel de police judiciaire, dans l'exercice des missions définies à l'article 14 du code de procédure pénale ; - Les militaires de la gendarmerie nationale ou les fonctionnaires de la police nationale habilités à effectuer des contrôles routiers, en application des dispositions du code de la route et du code de procédure pénale ; - Le personnel de police judiciaire adjoints et les gardes champêtres ; - Les fonctionnaires habilités à constater des infractions au code de la route. Sont destinataires* de tout ou partie des données à caractère personnel et informations mentionnées à l'article 3 : - La personne physique ou morale mise en cause, sa défense ou son ou sa mandataire ; - Les sociétés ayant pour activité la location de véhicules, uniquement en ce qui concerne les éléments d'identification du véhicule ; - Les sociétés, établissements ou administration mettant des véhicules à disposition de leurs collaborateurs ou clients et ayant signé une convention avec le Centre national de traitement, uniquement en ce qui concerne les éléments d'identification du véhicule ; - Le personnel de police judiciaire, les personnels de police judiciaire adjoints, les fonctionnaires auxquels sont attribuées par la loi certaines fonctions de police judiciaire, dans la limite de leurs habilitations légales ; les préfets pour l'exercice de leurs compétences en matière de circulation des véhicules ; les agents des services centraux placés sous l'autorité du ministre de l'intérieur chargés de l'application des dispositions de l'article L. 225-1 du code de la route ; les agents des services de la direction générale des finances publiques compétents pour le recouvrement des amendes dans la limite de leurs habilitations légales. Les données conservées dans le traitement peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers répondant aux conditions prévues au II de l'article 3 ainsi qu'aux autorités étrangères avec lesquelles il existe un accord d'échange d'informations relatives à l'identification du titulaire du certificat d'immatriculation. Pour les autres infractions faisant l'objet d'une procédure d'amende forfaitaire : Ont accès à tout ou partie des données à caractère personnel et informations mentionnées à l'article 3, à raison de leurs attributions et dans la limite du besoin d'en connaître : - Les personnels du Centre national de traitement et de l'Agence nationale de traitement automatisé des infractions pour l'exercice de leur compétence ;

	- Les autorités judiciaires ; - Les militaires de la gendarmerie nationale ou les fonctionnaires de la police nationale pour le traitement des infractions et l'exercice des prérogatives qui leur sont fixées par les dispositions du code de procédure pénale ; - Le personnel de police judiciaire, de police judiciaire adjoints, les fonctionnaires et personnels auxquels sont attribués par la loi certaines fonctions de police judiciaire, dans la limite de leurs habilitations légales ; Sont destinataires* de tout ou partie des données à caractère personnel et informations mentionnées à l'article 3 : - La personne physique ou morale mise en cause, sa défense ou sa ou son mandataire ; - Le personnel de la direction générale des finances publiques compétent pour le recouvrement des amendes dans la limite de leurs habilitations légales. Les données conservées dans le traitement peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers répondant aux conditions prévues au II de l'article 3. (Article 4 de l'arrêté du 13 octobre 2004)
Durée de conservation des données	Les données à caractère personnel et informations mentionnées à l'article 4 sont conservées pour une durée qui ne peut excéder : - 10 ans pour les délits ; - 10 ans pour les contraventions prévues par le code de la route ; - 5 ans pour les autres contraventions. Ces délais s'appliquent sans préjudice de la possibilité pour le contrevenant ou le mis en cause de demander au procureur de la République territorialement compétent d'ordonner l'effacement des données le concernant lorsque la procédure le concernant a donné lieu à une décision définitive de relaxe, de classement sans suite ou, lorsqu'il s'agit d'infractions relatives à la circulation routière, qu'il a récupéré le nombre de points ayant été retirés de son permis de conduire. (Article 3 de l'arrêté du 13 octobre 2004) Ainsi, si l'infraction est levée ou que la personne a purgé sa peine, ses données ne sont pas effacées automatiquement. Les opérations de collecte, de modification, de consultation, de communication et d'effacement des données à caractère personnel et informations font l'objet d'un enregistrement comprenant l'identifiant de l'auteur, la date, l'heure et la nature de l'opération. Ces informations sont conservées pendant 1 an. (Article 7-1 de l'arrêté du 13 octobre 2004)
Interconnexion avec d'autres fichiers ?	Dans le cadre des finalités prévues à l'article 1er et sous réserve du respect des dispositions de l'article 4, le présent traitement peut faire l'objet d'**interconnexion, mise en relation ou rapprochement*** avec : - Le fichier national des immatriculations ; - Le système national des permis de conduire ; - Le traitement automatisé de suivi du recouvrement des amendes et des condamnations pécuniaires ; - Les traitements relatifs à la gestion des contrats de location et des véhicules loués mis en œuvre par les sociétés ayant pour activité la location de véhicules, dans les conditions prévues par une convention signée avec le Centre national de traitement du contrôle automatisé ; - Les traitements relatifs à la gestion du parc automobile mis en œuvre par les sociétés ou établissements mettant des véhicules à disposition de leurs collaborateurs ou clients, dans les conditions prévues par une convention signée avec le Centre national de traitement du contrôle automatisé ; - Les systèmes de télépaiement des amendes mis en œuvre par les services compétents de la direction générale des finances publiques ; - Le traitement automatisé relatif au traitement des ordonnances pénales et des jugements devant les tribunaux de police dénommé « Minos » ; - Le traitement automatisé relatif aux procédures judiciaires au sein des tribunaux judiciaires dénommé « Cassiopée » ; - Le traitement dénommé « numérisation des procédures pénales » ; - L'application de gestion centrale ; - Le système d'immatriculation des véhicules ; - La base satellite des véhicules volés ; - Le TAJ ; - Le fichier des véhicules terrestres à moteur assurés. (Article 5 de l'arrêté du 13 octobre 2004)

	- Pour les infractions à la **circulation routière** : Les données conservées dans le traitement peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers répondant aux conditions prévues à l'article 3 ainsi qu'aux autorités étrangères avec lesquelles il existe un accord d'échange d'informations relatives à l'identification du titulaire du certificat d'immatriculation. - Pour les autres infractions faisant l'objet d'une **procédure d'amende forfaitaire** : Les données conservées dans le traitement peuvent être transmises à des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers répondant aux conditions de l'article 3 de l'arrêté du 13 octobre 2004. (Article 4 de l'arrêté du 13 octobre 2004)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas au présent traitement. (Article 7 de l'arrêté du 13 octobre 2004) Les droits d'information, d'accès, de rectification, d'effacement et à la limitation s'exercent directement auprès du Centre national de traitement du contrôle automatisé : formulaire de contact. Le droit d'accès au cliché pris par les appareils de contrôle automatique des infractions visées à l'article 1er s'effectue, par envoi, par courrier simple et à la demande expresse du titulaire du droit d'accès, sous le contrôle d'un officier ou agent de police judiciaire. La rectification des informations nominatives figurant sur le cliché pris par les appareils de contrôle automatique des infractions visées à l'article 1er peut être ordonnée par décision définitive des tribunaux compétents. (Article 6 de l'arrêté du 13 octobre 2004)
Remarques	Avant la modification du texte de loi régissant le fichier, les policiers et gendarmes utilisaient déjà le fichier comme base de données pour enregistrer les infractions de 4e catégorie, c'est-à-dire les infractions liées au non-respect du confinement par exemple. Si un individu répète 4 fois en moins d'un mois la même infraction alors celle-ci devient un délit, l'individu peut encourir de la prison. Le 9 avril 2020, Me Cassette a défendu un récidiviste qui n'a pas respecté le confinement devant le Tribunal judiciaire. Le journal Le Monde publie en 2020 un article sur l'affaire et la découverte du détournement du fichier: « *Me Cassette s'est rendu compte que, pour constater la réitération de l'infraction, les policiers et gendarmes consultaient un fichier, baptisé ADOC (pour Accès au dossier des contraventions), sur lequel les verbalisations électroniques de son client avaient été enregistrées. Or ce fichier créé par un arrêté du 13 octobre 2004 était destiné aux infractions routières et non pour les contraventions de 4e catégorie (135 euros).* » Maître Cassette a donc prouvé que la finalité du fichier avait été détournée ; une nullité de procédure a été reconnue, l'individu a été relaxé. Le 16 avril 2020 (soit 15 jours après l'affaire) un arrêté est publié au Journal officiel modifiant l'arrêté du 13 octobre 2004, rendant légal l'utilisation élargie que faisaient les policiers et gendarmes du fichier ADOC.
Textes qui régissent ce fichier	- Articles 495-17, R. 48-1 et D. 49-3 du code de procédure pénale - Articles L. 121-3, L. 130-9 et R. 130-11 du code de la route - Arrêté du 13 octobre 2004 portant création du système de contrôle automatisé - Arrêté du 14 avril 2020 modifiant l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé - Avis de la Commission nationale de l'informatique et des libertés en date du 9 avril 2020, sur un projet d'arrêté modifiant l'arrêté du 13 octobre 2004 portant création du système de contrôle automatisé (demande d'avis n° 19022550) - 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
Sources	Voir ci-dessus les « Textes qui régissent ce fichier » Jean-Baptiste Jacquin et Nicolas Chapuis, « Coronavirus : un fichier de police détourné pour repérer les récidivistes qui violent le confinement », Le Monde, avril 2020 La Quadrature du Net, « Fichage policier : recours contre le détournement du fichier du "Système de contrôle automatisé" », novembre 2020 Perot June [Brèves], « Non-respect des mesures de confinement et réitération : le périmètre contraventionnel du fichier « SCA » élargi dans l'urgence », La lettre juridique, avril 2020

Nom du fichier	**SETRADER**
Sens de l'acronyme	Système européen de traitement des données d'enregistrement et de réservation
Date de création	11 avril 2013
Quelle échelle ?	Nationale
Objectifs officiels	Le fichier a pour finalité : - « *la prévention, la répression de l'immigration clandestine et le contrôle aux frontières ;* - *la prévention et la répression des actes de terrorisme et des atteintes aux intérêts fondamentaux de la Nation.* » (Article 1 de l'arrêté du 11 avril 2013)

Objectif implicite	Le contrôle ciblé des personnes en provenance ou à destination de pays jugés comme « *présentant une sensibilité particulière en matière de risque terroriste ou d'immigration irrégulière* ». (Délibération n° 2013-016 du 17 janvier 2013)
Contenu des données	Les données à caractère personnel et informations relatives aux passagers aériens enregistrées dans le traitement prévu à l'article 1er sont les suivantes : - numéro et type du document de voyage utilisé ; - nationalité, nom, prénom, date de naissance, sexe ; - point de passage frontalier utilisé pour entrer sur le territoire français ou en sortir ; - code de transport (numéro du vol et code du transporteur aérien) ; - heures de départ et d'arrivée du transport ; - point d'embarquement et de débarquement ; - date du vol ; - point de départ et d'arrivée du vol ; - date d'expiration du document de voyage ; - statut de la personne embarquée (membre d'équipage, passager ayant pris un vol d'apport, passager ayant un vol de continuation, passager n'ayant pas eu de vol d'apport ni n'ayant de vol de continuation, passager ayant eu un vol d'apport et ayant un vol de continuation) ; - nombre, poids et identification des bagages ; - numéro de siège ; - Etat ou organisation émetteur du document de voyage ; - code repère du dossier passager ; - mention « connu » ou « inconnu » au fichier des personnes recherchées ainsi que dans le système d'information Schengen ; - nombre total des personnes transportées dans l'aéronef. (Article 2 de l'arrêté du 11 avril 2013)
Critères d'inscription dans ce fichier	Être une personne voyageant en avion, à destination ou en provenance d'un « *pays présentant une sensibilité particulière en matière de risque terroriste ou d'immigration irrégulière* ». La liste des pays n'est pas publiée. (Délibération n° 2013-016 du 17 janvier 2013)
Autorité(s) compétente(s)	Le directeur général de la police nationale (Article 8 de l'arrêté du 11 avril 2013)
Qui a accès à ce fichier ?	Peut accéder aux données le personnel individuellement désigné et dûment habilité : - des services centraux de la direction nationale de la police aux frontières ; - des directions de la police aux frontières des aérodromes parisiens ; - des services territoriaux de la police nationale chargés de la police aux frontières ; - de la sous-direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la direction du renseignement de la préfecture de police ; - du service central de renseignement criminel de la gendarmerie nationale ; - des services territoriaux du ministère du budget chargés de la lutte contre l'immigration irrégulière dont les agents sont individuellement désignés et spécialement habilités par le directeur régional des douanes et droits indirects ou, le cas échéant, par le directeur général des douanes et droits indirects ; - de la direction nationale du renseignement territorial et les services territoriaux de la police nationale chargés du renseignement territorial, aux seules fins de la prévention des actes de terrorisme ; - de la sous-direction antiterroriste de la direction nationale de la police judiciaire ; - de l'office central de lutte contre le crime organisé ; - de l'office central pour la répression de la grande délinquance financière ; - de l'office de lutte contre le trafic illicite de migrants ; - de l'office anti-cybercriminalité ; - des services centraux et territoriaux spécialement chargés de la prévention et de la répression des actes de terrorisme et des atteintes aux intérêts fondamentaux de la Nation de la direction générale de la sécurité intérieure ; - de la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialités violentes de la direction du renseignement de la préfecture de police ; - de la sous-direction des brigades centrales de la direction régionale de la police judiciaire de Paris ; - du service central de renseignement criminel de la gendarmerie nationale ; - de l'office central de lutte contre les atteintes à l'environnement et à la santé publique ; - des sections de recherches de la gendarmerie des transports aériens et de la gendarmerie de l'air et de l'espace ;

	- du bureau de la lutte antiterroriste de la sous-direction de la police judiciaire ; - de la direction nationale du renseignement et des enquêtes douanières (direction du renseignement douanier) ; - des services territoriaux en charge directement de la sûreté des transports internationaux ; - de l'office national anti-fraude, aux seules fins de la répression des actes de terrorisme entrant dans le cadre de ses attributions légales ; - des services de renseignement du ministère de la défense, dont les agents sont individuellement désignés et spécialement habilités par les directeurs de ces services, aux seules fins de prévention des actes de terrorisme et des atteintes aux intérêts fondamentaux de la Nation et dans la limite du besoin d'en connaître. (Annexe de l'arrêté du 11 avril 2013) Consultation des données : - Dans le cadre de la prévention et de la répression de l'immigration irrégulière, ces données peuvent être consultées pendant une durée de 6 mois à compter de leur transmission. - Dans le cadre du contrôle aux frontières extérieures, ces données peuvent être consultées pendant une durée de 24 heures à compter de leur transmission. Par exception, cette durée est portée à 12 jours pour les données à caractère personnel relatives aux personnes concernées par les seuls cas suivants : vols retardés, vols déroutés, usage de billets découplés, présentation à l'entrée du territoire après un certain délai, maintien en zone d'attente, refus d'entrée, procédure d'amende au transporteur. (Article 4 de l'arrêté du 11 avril 2013)
Durée de conservation des données	Les données enregistrées dans le fichier sont conservées 5 ans. Toutefois, la mention « connu » du FPR ou du N-SIS, est supprimée après 24h d'inscription de la personne dans le fichier. (Article 4 de l'Arrêté du 11 avril 2013)
Échange de données	Interconnexion avec le FPR et le N-SIS.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès et de rectification des données s'exercent directement auprès de la direction nationale de la police aux frontières du ministère de l'intérieur à l'adresse suivante : direction centrale de la police aux frontières, 8, rue de Penthièvre, 75008 Paris. Par exception, ces droits s'exercent auprès de la Cnil pour la mention « connu » ou « inconnu » au fichier des personnes recherchées ainsi que dans le système d'information Schengen. (Article 6 de l'arrêté du 11 avril 2013)
Remarques	Le système SETRADER ne concerne pas tous les vols français. Selon la Cnil, il ne concerne que les vols à destination ou en provenance de « *pays présentant une sensibilité particulière en matière de risque terroriste ou d'immigration irrégulière* ». Cette liste de pays concernés, émise par le ministère de l'intérieur, n'est pas publiée. En 2013, elle concernait une trentaine de pays n'appartenant pas à l'UE. Dans une nouvelle délibération de la Cnil datant du 19 avril 2018, il n'est pas précisé le nombre de pays concernés. De plus, le SETRADER permet à la police aux frontières de débuter son contrôle avant même l'arrivée des personnes aux contrôles en aéroport. En effet « *le traitement SETRADER permet aux autorités chargées d'effectuer les contrôles aux frontières de recevoir, à l'issue de l'enregistrement et avant le départ du vol, les données API détenues par les transporteurs aériens afin de faciliter l'exécution de ce contrôle, notamment en vérifiant que les voyageurs ne sont pas inscrits dans le fichier des personnes recherchées* ».(Délibération n° 2013-016 du 17 janvier 2013) L'incubateur des services numériques (DINUM) a réalisé une investigation en avril 2024 pour constater les difficultés rencontrées par les services de la PAF dans l'utilisation du SETRADER. Selon leurs conclusions : « *SETRADER : L'outil est simple d'utilisation mais obsolète (couverture incomplète, non-conformité, non maintenabilité), il est donc délaissé par certains services* ». De plus, « *SETRADER ne peut être maintenu sur la durée et ne permet plus d'anticiper efficacement les contrôles dans les points de passages frontaliers (PPF) aériens.* ». Il serait davantage conseillé après investigation, de former les services de la PAF à l'API-PNR que de continuer à utiliser le SETRADER.
Textes qui régissent ce fichier	- Arrêté du 11 avril 2013 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé SETRADER - Délibération n° 2013-016 du 17 janvier 2013 - Délibération n° 2018-139 du 19 avril 2018 portant avis sur un projet d'arrêté modifiant l'arrêté du 11 avril 2013 relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé SETRADER - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » ANDV – Aérien, Aide au contrôle frontière Beta.gouv.fr

Nom du fichier	**SILCF**
Sens de l'acronyme	Système informatisé de lutte contre les fraudes
Date de création	1er juillet 2003
Quelle échelle ?	Nationale
Objectif officiel	La direction générale des douanes et droits indirects met en œuvre un traitement automatisé comportant des informations nominatives dénommé 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 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 7 novembre 2012)
Objectif implicite	Le fichier étant interconnecté avec API-PNR, il revient également à contrôler les déplacements aériens des personnes. Le traitement DALIA[23] alimente en temps réel le fichier SILCF à l'issue de la validation du formulaire électronique par la personne déclarante. Ce traitement permet aux personnes de s'acquitter par internet de leur obligation déclarative de transferts d'argents entre métropole et outre-mer en provenance ou vers d'autres pays de l'UE ou pays dit tiers. Ainsi, avec le traitement automatique DALIA et avec l'interconnexion avec le fichier API-PNR, le fichier SILCF est un moyen de contrôle des déplacements financiers et physiques.
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 Pour le personnel des douanes : nom, prénom, fonctions et données d'identification au sein de l'organisation administrative (Article 3 de l'arrêté du 7 novembre 2012)
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 ;

[23] Le traitement DALIA n'est pas développé dans cette boîte à fichiers car les textes de loi le régissant ont été abrogés le 30 janvier 2025.

	- 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 à l'Article 2 de l'arrêté du 7 novembre 2012
Autorité(s) compétente(s)	La direction générale des douanes et droits indirects
Qui a accès à ce fichier ?	Peuvent se connecter au SILCF en 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 le personnel de la direction générale des douanes et droits indirects : - Le personnel dûment habilité 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, le personnel des services ayant signalé un risque de fraude conserve la possibilité d'accéder aux informations relatives à ce signalement ; - Le personnel dûment habilité des services d'enquête sont destinataires* des informations relatives aux enquêtes qui leur sont confiées. Le personnel des autres services sont informés qu'une personne fait l'objet d'une demande d'enquête ; - Toutes les agentes et agents, y compris ceux 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 ; - Le personnel habilité des laboratoires des douanes sont destinataires* des demandes d'analyse et d'expertise de marchandises qui leur sont confiées ; - Le personnel dûment habilité 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 ; - Le personnel dûment habilité 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, le personnel dûment habilité 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. (Article 6 de l'arrêté du 7 novembre 2012)
Durée de conservation des données	- 3 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). - 10 ans pour les informations nominatives relatives aux fraudes constatées, à compter de l'année de la constatation. - 5 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 5 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)
Échanges de données	Interconnexion avec API-PNR, non écrite sur l'arrêté régissant le SILCF mais sur la fiche explicative du fichier API-PNR sur le site la Cnil. Échanges de données avec d'autres fichiers non connus.
Quelle échelle ?	Nationale

Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. (Article 10 de l'arrêté du 1er juillet 2003) Les droits d'accès et de rectification 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'État, 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 Cnil. 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 l'arrêté du 1er juillet 2003)
Textes 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 - 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 - Arrêté du 1er 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 - Délibération n° 03-029 du 22 mai 2003 de la Cnil concernant la création par la direction générale des douanes et droits indirects d'un système d'information de lutte contre la fraude - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir ci-dessus « Textes qui régissent ce fichier » Cnil, Fiche explicative du "système API-PNR"

Nom du fichier	**TAJ**
Sens de l'acronyme	Traitement d'antécédents judiciaires (Il remplace les anciens fichiers STIC - système de traitement des infractions constatées et JUDEX - système judiciaires de documentation et d'exploitation) Le TAJ est alimenté via l'application* GASPARD NG, qui permet d'alimenter simultanément le TAJ et le FAED. Le TAJ contient le logiciel* de reconnaissance faciale FaceVACS-DBScan de la société COGNITEC.
Date de création	4 mai 2012
Quelle échelle ?	Nationale
L'application* GASPARD NG	Comme le précise la Caisse de solidarité de Lyon dans La folle volonté de tout contrôler : **GASPARD-NG** (« gestion automatisée des signalements et des photographies anthropométriques* répertoriés et distribuables nouvelle génération ») est un logiciel, dont l'utilisation n'est pas reconnue par les services de police. Avec des objectifs similaires, GASPARD puis GASPARD-NG semblent toutefois exister depuis au moins 2008. Lors d'un reportage de Mediapart sur la police technique et scientifique, le logiciel* GASPARD-NG apparaît à l'écran d'un agent de police (Deux millions de contrôles au faciès » OWNI, News, Augmented). On peut en déduire que les données collectées sont (au moins) : le type ethnique, la pilosité, les yeux, les cheveux, les signes particuliers, les accents, la forme du visage et des photos. Dans sa plainte, la Quadrature du Net cite un rapport qui recense les outils de la police : « *L'outil GASPARD-NG permet aussi d'alimenter le TAJ des photographies des mis en cause. Il est ainsi désormais possible de lancer dans le TAJ des recherches à partir d'une photographie. Les résultats de la recherche font apparaître les photographies déjà présentes susceptibles d'y correspondre en fonction d'un certain nombre de paramètres (écartement des yeux, etc.). La recherche peut ailleurs être affinée par certains critères, tels que le sexe, la couleur des yeux ou des cheveux, etc. Le TAJ constitue déjà, de ce point de vue, un outil de reconnaissance faciale.* » (Plainte collective contre la Technopolice – Technopolice) Selon la Caisse de solidarité de Lyon dans La folle volonté de tout contrôler : « *On peut légitimement supposer que c'est l'outil GASPARD-NG qui permet d'effectuer des rapprochements biométriques* entre des photos extraites d'une vidéo où des infractions seraient commises par exemple, et les fiches photographiques du TAJ.* »
Le logiciel* de reconnaissance faciale FaceVACS-DBScan	**Le logiciel* FaceVACS-DBScan** est en lien avec le logiciel* GASPARD-NG et le TAJ. Il est commercialisé par la société allemande COGNITEC, permet depuis 2020 d'opérer des recherches « en quelques secondes », mais également d'effectuer des comparaisons avec des photographies, images et vidéos, dont celles, de moindre qualité, issues des réseaux sociaux.

Objectifs officiels	Selon la Cnil, le TAJ est constitué des données recueillies notamment par la police, la gendarmerie nationale et les agents des douanes habilités à exercer des missions de police judiciaire. 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) Le fichier TAJ a pour objectif de faciliter : - La constatation des infractions ; - Le rassemblement des preuves de ces infractions ; - Et la recherche de leurs auteurs. (Article 230-6 du code de procédure pénale) Ce traitement a également pour objet l'exploitation des informations recueillies à des fins de recherches statistiques.
Objectifs implicites	Selon Marc Duranton et Jean-Philippe Foegle, ce fichier a une visée sécuritaire au détriment notamment du droit au respect de la vie privée.
Contenu des données	Personnes mises en causes en tant qu'auteures ou complices d'une infraction : - 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 Concernant les victimes : - 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 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 : - 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) (Article R. 40-26 du code de procédure pénale)
Critères d'inscription dans ce fichier	Toutes les personnes, sans limitation d'âge, concernées par : - Les personnes à l'encontre desquelles sont réunis, lors de l'enquête préliminaire, de l'enquête de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime, d'un délit ou d'une contravention de cinquième classe prévue aux articles R. 625-1 à R. 625-3, R. 625-7, R. 625-9, R. 635-1, R. 635-3 à R. 635-5, R. 645-1, R. 645-2 et R. 645-5 à R. 645-15 du code pénal ; - 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 au sens des articles 74 et 74-1. (Article R. 40-25 du code de procédure pénale)
Autorité(s) compétente(s)	Le ministre de l'intérieur (direction générale de la police nationale et direction générale de la gendarmerie nationale)
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 ou de titre de séjour : - Les policiers et policières des services de la police nationale exerçant des missions de police judiciaire ; - Les militaires des unités de la gendarmerie nationale exerçant des missions de police judiciaire ; - Le personnel de l'Office national anti-fraude ; - Les douanes ; - Les magistrats du parquet ; - Les agents et agentes des services judiciaires ; - Le magistrat, chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel ; - Les agents des unités de la gendarmerie nationale exerçant des missions de police.

	Peuvent être destinataires* des données : - Les autres personnels de l'État investis par la loi d'attribution de police judiciaire ; - Les magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis ; - Les organismes de coopération internationale en matière de police judiciaire ; - Les services de police étrangers. (Article R. 40-28 du code de procédure pénale) Dans le cadre de certaines enquêtes et habilités, peuvent accéder aux données les personnels : - De la police et la gendarmerie ; - Des services spécialisés de renseignement ; - Du service à compétence nationale dénommé « Service national des enquêtes administratives de sécurité » ; - Du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire » ; - Investis de missions de police administrative. (Article R. 40-29 du code de procédure pénale)
Durée de conservation des données	La durée de conservation des 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 a 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 recherche 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. Voir la liste des infractions permettant de conserver 40 ans les données concernant les personnes mises en cause majeures à l'article R. 40-27 du code de procédure pénale
Échanges de données	Interconnexion avec ACCReD. Dans le cadre des engagements internationaux en vigueur, le TAJ est également constitué des données à caractère personnel issues des traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers. Cela signifie une interconnexion avec EUROPOL et INTERPOL. (Article R. 40-29 du code de procédure pénale) Selon la Cnil : Une interconnexion avec les traitements de rédaction des procédures de la police et de la gendarmerie nationales (LRPPN[24] et LRPGN[25]), le logiciel* de rédaction des procédures des douanes judiciaires (LRPDJ[26]) et le traitement CASSIOPÉE[27] est prévue pour l'alimentation automatique du TAJ.

[24] Le logiciel de Rédaction des Procédures de la Police Nationale alimente automatiquement le TAJ, FOVeS et CASSIOPEE, et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer dans le présent document au vu de sa proximité avec le TAJ et le FAED. Voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

[25] Le logiciel de Rédaction des Procédures de la Gendarmerie Nationale alimente automatiquement le TAJ, FOVeS et CASSIOPEE, et échange des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED). Il a été décidé de ne pas l'intégrer dans le présent document au vu de sa proximité avec le TAJ et le FAED. Voir Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024, p. 49.

[26] Le logiciel de Rédaction des Procédures de la Douane Judiciaire a « *pour finalité l'aide à la rédaction des actes de procédure judiciaire établis par les agents du service d'enquêtes judiciaires des finances (SEJF) afin d'assurer la clarté et l'homogénéité de la rédaction des procédures qu'ils mettent en œuvre et de permettre la collecte des informations nécessaires à la conduite de ces procédures, en vue de leur exploitation et de leur transmission à l'autorité judiciaire compétente* ». Il a été décidé de ne pas l'intégrer dans le présent document au vu de sa proximité avec le TAJ et le FAED. Pour plus d'informations, voir le site Impots.gouv.

[27] CASSIOPÉE est la chaîne applicative supportant le système d'information orienté procédure pénale et enfants qui est prévue aux articles 48-1 et R. 15-33-66-4 du code de procédure pénale. Les données sont accessibles par les juges, les procureurs/procureures, greffiesr/greffières, éducateurs/éducatrices de la protection judiciaire de la jeunesse. Il n'a pas semblé central dans le cadre de cette boîte à fichiers qui recense les fichiers de contrôle des personnes étrangères (par accès direct* ou accès indirect*), d'où le fait qu'il n'a pas fait l'objet d'une fiche détaillée.

	Échange de données avec le fichier FAED.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. (Article R. 40-33 du code de procédure pénale) Droit d'accès et de rectification direct auprès du : ministère de l'intérieur, Place Beauvau (75018 Paris) – procédure disponible sur Traitement d'antécédents judiciaires (Taj) | Service-Public.fr Le ministère a 2 mois pour répondre. Droit d'accès et de rectification indirects : 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 mises en cause, autre possibilité : adresser une requête par lettre recommandée avec accusé de réception (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* du 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'1 mois à compter de l'envoi de la décision de refus. (Article 230-8 du code de procédure pénale) Un magistrat peut également agir d'office ou sur requête des particuliers. Il dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles dans les traitements mentionnés au premier alinéa du présent article que le procureur de la République. Lorsque la personne concernée le demande, la rectification pour requalification judiciaire est de droit. Il se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai de 2 mois. Il dispose, pour l'exercice de ses fonctions, d'un accès direct* à ces traitements automatisés. Les décisions de ce magistrat en matière d'effacement ou de rectification des données à caractère personnel sont susceptibles de recours devant le président de la chambre de l'instruction de la cour d'appel de Paris. (Article R. 40-31 du code de procédure pénale)
Remarques	En 2018, 87 millions d'affaires répertoriées dans le TAJ, et plus de 18,9 millions de fiches de personnes mises en cause. En 2021, la police procédait en moyenne à 1 680 reconnaissances faciales par jour (Plainte collective contre la Technopolice – Technopolice). Le TAJ peut être consulté au cours d'une enquête de police, mais aussi au cours d'une enquête administrative pour l'accès à certaines professions (agent de police, gardiennage, surveillance, militaire, secteur du nucléaire, intervention dans des grands événements, (par exemple les Jeux Olympiques), etc.) et **lors des demandes de titre de séjour et de nationalité française**. Pour les mineurs, l'avocat peut demander que le TAJ ne soit pas consulté dans le cadre des enquêtes administratives. (Article L. 634-1 du code de la justice pénale des mineurs) De plus, comme analysé dans le travail de La Caisse de solidarité de Lyon dans La folle volonté de tout contrôler : « *depuis novembre 2019, la reconnaissance faciale peut être utilisée à partir de n'importe quelle photographie (surveillances, images postées sur les réseaux sociaux, glanées sur internet, ou provenant de vidéos). La reconnaissance faciale peut ainsi être mise en œuvre à partir de photographies prises par les policiers et les gendarmes, en particulier à partir des tablettes NEOPOL (police) et NEOGEND (gendarmerie)[28]. Par conséquent, il est techniquement facile, au cours d'un contrôle d'identité, de prendre en photo une personne avec NEO, de verser sa photographie dans le TAJ, et d'exécuter le logiciel* de reconnaissance faciale pour retrouver son identité*. » Cette pratique semble exister sans fondement légal. En effet, la prise de photographie (de même que la prise d'empreintes) au cours d'une vérification d'identité ne peut se faire que dans un cadre précis : - Refus de décliner son identité ou éléments d'identité manifestement inexacts, - Autorisation nécessaire du procureur ou du juge d'instruction, - Rédaction d'un procès-verbal qui justifie le contrôle et informe la personne de ses droits (etc.).

[28] Les tablettes « NEO » sont mises en place depuis 2015. Selon un avis relatif au projet de loi de finances n° 3360 du député Stéphane Mazars datant du 13 octobre 2020, l'objectif est de « moderniser les forces en leur permettant d'avoir accès, en mobilité, à la plupart des outils dont ils ne disposaient auparavant qu'au sein du commissariat ou de la gendarmerie ». Avec ces tablettes, il est possible de consulter et d'enregistrer des données sur différents fichiers.

	Le 26 avril 2022, le Conseil d'État, saisi par la Quadrature du Net qui demandait la suppression de la reconnaissance faciale dans le TAJ, a jugé que celle-ci était légale et a rejeté le recours. (Conseil d'État, 26 avril 2022, n° 442364) La Quadrature du net a déposé un nouveau recours, cette fois sous la forme d'une plainte collective auprès de la Cnil en septembre 2022 concernant la vidéosurveillance, le fichage de masse et la reconnaissance faciale. Cette plainte est toujours en cours. (Voir La Quadrature du Net porte plainte contre la « technopolice » du ministère de l'intérieur - Next) En 2024, la Cnil a rappelé à l'ordre le ministère de l'intérieur et des outre-mer et le ministère de la Justice pour leur mauvaise gestion du fichier TAJ. Elle dénonce les manquements à la loi informatique et liberté, notamment concernant la conservation des données, l'absence d'information des personnes concernées et l'absence de prise en compte des droits des personnes concernées. (Cnil, *« Traitement d'antécédents judiciaires : la CNIL rappelle à l'ordre deux ministères »*, 2024)
Textes qui régissent ce fichier	- Articles R. 40-23 à R. 40-34 et articles 230-6 à 230-11 du code de procédure pénale - Article L. 634-1 du code de la justice pénale des mineurs - Conseil d'État, 26 avril 2022, n° 442364 - Décret n° 2024-302 du 2 avril 2024 portant adaptation du code de procédure pénale et d'autres dispositions réglementaires à la création de l'Office national anti-fraude et d'agents de police judiciaire des finances Décret n° 2021-682 du 27 mai 2021 portant partie réglementaire du code de la justice pénale des mineurs (articles en R) - Décret n° 2018-687 du 1er 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 - Décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires - Délibération n°SAN-2024-017 du 17 octobre 2024 de la Cnil - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, Voir « Textes qui régissent ce fichier » ci-dessus Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 Cnil, « TAJ : Traitement d'Antécédents Judiciaires », 2018 Cnil, « Traitement d'antécédents judiciaires : la CNIL rappelle à l'ordre deux ministères », 2024 Duranton Marc et Foegle Jean-Philippe, « Fichage partout, oubli nulle-part ? Le Conseil d'État ouvre un boulevard au fichier Taj », Actualités droits et libertés, juillet 2014 Manach Jean-Marc, La Quadrature du Net porte plainte contre la « technopolice » du ministère de l'intérieur, Next, 2022

Nom du fichier	**Table de correspondance des noms et prénoms**
Sens de l'acronyme	Traitement automatisé de données à caractère personnel dénommé « table de correspondance des noms et prénoms »
Date de création	19 décembre 2023
Quelle échelle ?	Nationale
Objectifs officiels	Le fichier a pour finalité « *la consultation de l'identité des personnes ayant changé de nom ou de prénom en application des articles 60, 61 et 61-3-1 du code civil et la mise à jour de cette identité dans les traitements de données à caractère personnel que lui-même ou les établissements publics qui lui sont rattachés mettent en œuvre* ». (Article 1 de l'arrêté du 19 décembre 2023)
Objectifs implicites	Pour plusieurs associations dont la Quadrature du Net : « *accessible par la police et présenté comme une simplification administrative, ce texte [Arrêté du 19 décembre 2023 portant création d'un traitement automatisé de données à caractère personnel dénommé « table de correspondance des noms et prénoms »] aboutit en réalité à la constitution d'un fichier plus que douteux, centralisant des données très sensibles, et propice à de nombreuses dérives* ». Le fichier recense, de fait, les personnes transgenres et une partie des personnes étrangères. (La Quadrature du Net, « La France crée un fichier des personnes trans », 2024)
Contenu des données	- Le nom de famille antérieur au changement de nom - Le nom de famille postérieur au changement de nom - Les prénoms antérieurs au changement de prénom

	- Les prénoms postérieurs au changement de prénom - La date et le lieu de naissance - La date du changement de nom ou de prénom - Le sexe - Le cas échéant, la filiation (Article 2 de l'arrêté du 19 décembre 2023)
Critères d'inscription dans ce fichier	Avoir réaliser un changement de nom et/ou de prénom administratif
Autorité(s) compétente(s)	Le ministère de l'intérieur
Qui a accès à ce fichier ?	Ont accès aux données : - Le personnel des services de la police nationale - Les personnels des unités de la gendarmerie nationale - Les agents et agentes des services centraux du ministère de l'intérieur et des préfectures et sous-préfectures - Les agents et agentes du service à compétence nationale dénommé « Service national des enquêtes administratives de sécurité » - Les agents et agentes du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire » - Les personnels du service à compétence nationale dénommé « Service national des enquêtes d'autorisation de voyage » - Les agents et agentes du Conseil national des activités privées de sécurité - Les agents et agentes du service à compétence nationale dénommé « Agence nationale des données de voyage » Dans la limite de leur désignation individuelle et de leur habilitation. (Article 4 de l'arrêté du 19 décembre 2023)
Durée de conservation des données	Maximum 6 ans à compter de leur enregistrement (Article 3 de l'arrêté du 19 décembre 2023)
Échanges de données	Les services de police peuvent consulter le RNIPP (répertoire national d'identification des personnes physiques) pour enregistrer des données dans le fichier « table de correspondance des noms et prénoms » (Loi n° 2022-301 du 2 mars 2022 relative au choix du nom issu de la filiation modifiant le décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès, de rectification et à la limitation des données s'exercent auprès du secrétariat général du ministère de l'intérieur. (Article 5 de l'arrêté du 19 décembre 2023)
Remarques	Les opérations de collecte, de modification, de consultation, de communication et d'effacement des données à caractère personnel et informations font l'objet d'un enregistrement. Les opérations de consultation et de communication établissent l'identifiant de l'auteur, la date, l'heure, la nature de l'opération et, le cas échéant, les destinataires des données. Ces informations sont conservées pendant un délai de 3 ans. (Article 6 de l'arrêté du 19 décembre 2023) Dans sa délibération du 5 octobre 2023, la Cnil considère qu'une analyse d'impact relative à la protection des données (AIPD) est nécessaire « eu égard aux risques élevés pour les droits et libertés pour les personnes concernées en cas de violation de ces données, notamment en ce que le traitement établit une liste exhaustive des personnes ayant changé de prénom en raison de leur genre ». (Délibération n° 2023-103 du 5 octobre 2023) Pour la Quadrature du Net « *En centralisant des informations, au demeurant très sensibles, l'État crée un double risque. D'une part,* ***que ces informations dès lors trop facilement accessibles soient dévoyées*** *et fassent l'objet de détournement et autres consultations illégales de la part de policiers, comme pour bon nombre de fichiers de police au regard du recensement récemment effectué par Mediapart. […] D'autre part, du fait de la centralisation induite par la création d'un fichier,* ***les sources de vulnérabilité et de failles de sécurité sont démultipliées*** *par rapport à un accès décentralisé à ces informations*. » (La Quadrature du Net, « La France crée un fichier des personnes trans », 2024) Dans une question écrite au ministère de l'intérieur, la député Sandra Regol a souligné les risques du fichier « *de porter atteinte aux droits fondamentaux des personnes trans, qu'il met directement en danger en rendant accessibles des informations relatives à leur transidentité* », notamment car il « *expose les personnes immigrées naturalisées qui souhaitent franciser*

	leur nom, comme les personnes trans, à des risques d'outing et de discriminations ». (Question n°7368 à l'Assemblée nationale : Grave préoccupation sur la table de correspondance des noms et prénoms, 10 juin 2025)
Textes qui régissent ce fichier	- Arrêté du 19 décembre 2023 portant création d'un traitement automatisé de données à caractère personnel dénommé « table de correspondance des noms et prénoms » - Délibération n° 2023-103 du 5 octobre 2023 portant avis sur un projet d'arrêté portant création d'un traitement automatisé de données à caractère personnel dénommé « Table de correspondance des noms et prénoms » - Loi n° 2022-301 du 2 mars 2022 relative au choix du nom issu de la filiation modifiant le décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire) - 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 - Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
Sources	Légifrance, voir la rubrique les « Textes qui régissent ce fichier » La Quadrature du Net, « La France crée un fichier des personnes trans », 2024 Question n°7368 à l'Assemblée nationale : Grave préoccupation sur la table de correspondance des noms et prénoms, 10 juin 2025

Nom du fichier	**TES**
Sens de l'acronyme	Titre électronique sécurisé En lien, du fait des démarches dématérialisée, avec le « Service de garantie de l'identité numérique » (SGIN) et son application
Date de création	28 octobre 2016
Quelle échelle ?	Nationale
L'application SGIN	Le SGIN est un « moyen d'identification électronique » mis en place par l'État. Peuvent accéder aux données dans le SGIN selon France identité.gouv.fr : - Le personnel des services du secrétariat général (Programme interministériel France identité numérique) et les agents de l'Agence nationale des titres sécurisés, chargés de la maîtrise d'ouvrage et de la maîtrise d'œuvre du traitement ; - Le personnel des services des responsables du traitement ; - Les usagers eux-mêmes lorsqu'ils obtiennent des attestations électroniques d'attributs d'identité. Peuvent recevoir les données à caractère personnel : - Le téléservice FranceConnect ; - Les fournisseurs de téléservices liés par convention à FranceConnect, auxquels FranceConnect transmet les données sans modification ; - Les fournisseurs de téléservices liés par convention aux responsables du traitement ; - Les personnes physiques ou morales auxquelles les usagers souhaitent transmettre une attestation électronique d'attributs d'identité. (France-Identité-AIPD-Synthèse) Le SGIN est associé au TAJ et au fichier DOCVERIF.
Le fichier DOCVERIF	Comme précisé dans La folle volonté de tout contrôler : Jusqu'en 2021, DOCVERIF ne recevait des informations du TES que lorsqu'une carte d'identité ou un passeport était déclaré perdu ou volé. Dorénavant, le TES transmet automatiquement à DOCVERIF les données de tous les passeports et toutes les cartes d'identité (sauf la photographie et les empreintes digitales). DOCVERIF devient donc un fichier-miroir du TES.
Objectifs officiels	Selon la Cnil, le fichier TES permet le regroupement, dans une base de données centralisée, de l'image numérisée du visage et des empreintes digitales (de chacun des index, sinon d'autres doigts) de l'ensemble des demandeurs de carte nationale d'identité et de passeport. Les objectifs officiels du fichier TES sont : - 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 modifié par décret n° 2024-689 du 5 juillet 2024)
Objectifs implicites	Selon la 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 sûreté 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) 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, « Fichier TES : danger pour les libertés », Communiqué de presse, 14 novembre 2016)
Contenu des données	Données 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 - Adresse de messagerie électronique et coordonnées téléphoniques lorsqu'il y a une pré-demande en ligne, ou envoi postal sécurisé ou sur déclaration de la personne - Dans le cas de l'envoi postal, le code de connexion délivré par l'administration Données 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 - Mention, avec la date, de l'invalidation du titre et de son motif (perte, vol, retrait, interdiction de sortie du territoire, autre motif), de la restitution du titre à l'administration, de sa destruction - Mentions des justificatifs présentés à l'appui de la demande de titre - Informations à caractère technique - Informations relatives à caractère technique - Informations relatives à la demande de titre - La date et le mode de remise de titre - Informations relatives à la réception du passeport 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
Critères d'inscription dans ce fichier	Avoir demandé la délivrance ou le renouvellement d'une carte nationale d'identité ou d'un passeport. (Article 1 du décret n° 2016-1460 du 28 octobre 2016)
Autorité(s) compétente(s)	La direction des libertés publiques et des affaires juridiques (ministère de l'intérieur) et par l'agence nationale des titres sécurisés (ANTS)
Qui a accès à ce fichier ?	Peuvent accéder aux données : - Le personnel des services centraux du ministère de l'intérieur et du ministère de l'Europe et des affaires étrangères chargés de l'application de la réglementation relative au passeport et à la carte nationale d'identité ; - Le personnel des préfectures et des sous-préfectures chargés de la délivrance des passeports et des cartes nationales d'identité ; - Le personnel diplomatique et consulaire chargé de la délivrance des passeports et des cartes nationales d'identité, individuellement désigné et dûment habilité par l'ambassadeur ou le consul ; - Les agents chargés de la délivrance des passeports de service au ministère de l'intérieur, individuellement désigné et dûment habilité par le ministre de l'intérieur ; - Le personnel de l'Agence nationale des titres sécurisés chargé de la mise en œuvre du traitement ; - Le personnel des communes individuellement désigné et dûment habilité par le maire ; - Pour les seuls passeports de mission, le personnel des formations administratives du ministère de la défense, individuellement désigné et dûment habilité par le ministre de la Défense. Peuvent accéder aux données à l'exclusion de l'image numérisée des empreintes digitales : - Le personnel 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 ; - Le personnel 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 ; - Le personnel 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 États 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. Les données peuvent être transmises aux autorités compétentes des États membres d'INTERPOL. (Articles 3 et 4 du décret du 28 octobre 2016)
Durée de conservation des données	La durée de conservation des données varie selon l'âge : - Pour les personnes mineures, les données sont conservées 10 ans. - Pour toute personne adulte demandeuse ou titulaire du titre, les données sont conservées dans le traitement pendant 15 ans. Et selon le titre demandé : - Les données relatives aux passeports de service et aux passeports de mission sont conservées pendant 10 ans. - Le délai court à compter de la délivrance du titre, ou, à défaut, à compter de l'enregistrement de la demande. Il est possible pour la personne concernée de demander à ce que l'image numérisée de ses empreintes ne soit pas conservée dans le traitement au-delà d'un délai de 90 jours à compter de la date de délivrance du titre ou de la date de refus de cette délivrance par le service instructeur, la copie sur papier des empreintes étant alors conservée par l'Agence nationale des titres sécurisés pour une durée de 15 ans. (Article 9 du décret du 28 octobre 2016)
Échanges de données ?	Interconnexion : Dans la délibération n° 2021-022 de la Cnil datant du 11 février 2021 : « *Le traitement TES a vocation à alimenter la partie nationale du Système d'information Schengen de deuxième génération (N-SIS II) [voir SIS II], ainsi que le traitement Stolen and Lost Travel Documents (SLTD) géré par Interpol, de données relatives aux titre perdus, volés ou invalidés. Cette alimentation, qui est réalisée de manière automatique, implique que le traitement TES transmette des données, à l'exception des données biométriques, dès lors qu'est enregistrée une déclaration de perte, ou de vol.* ». Il y a donc interconnexion avec le fichier SLTD (Interpol), le N-SIS (voir fiche SIS II).

	Dans la délibération n° 2024-099 de la Cnil datant du 12 décembre 2024 relatif au fichier DOCVERIF : « *pour assurer l'accès à ces informations, DOCVERIF est alimenté par une interconnexion […] pour les données relatives aux CNI et passeports, le traitement « titres électroniques sécurisés » (TES)* ». Interconnexion avec le logiciel de rédaction des procédures de la police nationale et le logiciel* de rédaction des procédures de la gendarmerie nationale. (Article 7-1 du décret n° 2016-1460 du 28 octobre 2016) De plus, avec la nouvelle carte d'identité, une consultation* automatique est faite avec au minimum le TAJ et le FPR est établie lors d'un contrôle d'identité par les tablettes NEOGEND (gendarmerie) et NEOPOL (police). Dans certaines conditions, les agents et agentes 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 et les agents et agentes des services spécialisés du renseignement pour « les besoins de la prévention et de la répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme » « *peut consulter le TES pour obtenir l'image d'une personne, la copier dans le TAJ et, à partir de là, traiter cette photo de façon automatisée pour la comparer à d'autres images, telles que celles prises par des caméras de surveillance* ». (La Quadrature du Net, La reconnaissance faciale des manifestant·es est déjà autorisée, 2019) Enfin, le fichier des personnes recherchées FPR est consulté au moment de la demande pour vérifier qu'aucun élément ne s'oppose à sa délivrance. (Article 8 du décret n° 2016-1460 du 28 octobre 2016)
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. (Article 12 du décret n° 2016-1460 du 28 octobre 2016) La personne demandant un titre est informée, au moment de la demande : - De la nature des données à caractère personnel enregistrées dans le traitement ; - Du nombre et de la nature des empreintes digitales enregistrées dans le traitement ; - De la possibilité qui lui est offerte, pour l'établissement d'une carte nationale d'identité, de refuser la conservation dans le traitement de l'image numérisée de ses empreintes digitales au-delà d'un délai maximal de 90 jours à compter de la date de délivrance du titre ou de la date de refus de délivrance par le service instructeur ; - S'il fait usage de la possibilité mentionnée au 3°, de la conservation d'une copie sur papier de l'image numérisée de ses empreintes digitales dans les conditions définies au I bis de l'article 4-3 du décret du 22 octobre 1955 ; - Des autres renseignements mentionnés à l'article 13 du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. La remise du passeport et de la carte nationale d'identité s'accompagne d'une copie sur papier des données nominatives enregistrées dans le composant électronique. (Article 10 du décret n° 2016-1460 du 28 octobre 2016) Le droit d'accès et le droit de rectification s'exercent auprès de l'autorité de délivrance dans les conditions prévues respectivement aux articles 13, 15, 16 et 18 du règlement (UE) 2016/679. Cependant, lorsque les informations sont enregistrées, il n'est pas possible par la suite de s'opposer à leur traitement ni d'en demander l'effacement, y compris pour les empreintes digitales. (Voir Le fichier des titres électroniques sécurisés (TES) | Cnil mis à jour en 2021)
Remarques	Même si la reconnaissance faciale est interdite dans le TES (Article 2 II du décret n° 2016-1460 du 28 octobre 2016), aucune disposition n'interdit l'utilisation de la reconnaissance faciale à partir des photographies contenues dans le TES. « *Ces accès au fichier engendrent donc des risques importants que la reconnaissance faciale soit utilisée par le versement de ces photographies dans un autre fichier de police (par exemple le Traitement des antécédents judiciaires, TAJ), qui, lui, permet la reconnaissance faciale ou sur réquisition de la photographie au cours d'une enquête* ». (La Quadrature du Net, Le fichier TES, prémisse à la reconnaissance faciale de masse, arrive devant le Conseil d'État, 2018) À compter du 2 août 2021, toute personne souhaitant se voir délivrer une carte nationale d'identité ou souhaitant faire renouveler sa carte nationale d'identité arrivée à expiration bénéficiera de la nouvelle CNI. Cette fiche tient compte des modifications apportées au fichier TES dans le cadre de cette évolution. (Le fichier des titres électroniques sécurisés (TES) | Cnil)
Textes qui régissent ce fichier	- 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

	- Décret n° 2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données* à caractère personnel dénommé « titres électroniques sécurisés » (TES) - Décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité - Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports - Délibération n° 2016-292 du 29 septembre 2016 de la Cnil 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 - 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 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Sources	Légifrance, voir la rubrique les « Textes qui régissent ce fichier » Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 CNCDH, Déclaration « Pour la suspension du fichier dit « Titres électroniques sécurisés » », 15 décembre 2016 Le site de l'Observatoire des libertés et du numérique, « Fichier TES : danger pour les libertés », Communiqué de presse, 14 novembre 2016 Cnil, Le fichier des titres électroniques sécurisés (TES) La Quadrature du Net, La reconnaissance faciale des manifestant·es est déjà autorisée, 2019 La Quadrature du Net, Le fichier TES, prémisse à la reconnaissance faciale de masse, arrive devant le Conseil d'État, 2018

Nom du fichier	**VISABIO**
Sens de l'acronyme	Visa biométrique
Date de création	3 novembre 2007
Quelle échelle ?	Nationale
Objectifs officiels	Ce fichier a pour objectifs de : - Mieux garantir le droit au séjour des personnes en situation régulière et lutter contre l'entrée et le séjour irréguliers des personnes étrangères 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 États 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 d'une frontière extérieure des États membres de l'espace Schengen ou d'une frontière des territoires français d'outre-mer : vérifier l'authenticité du visa et l'identité de la personne qui le détient ; - Lors des contrôles d'identité sur le territoire national : vérifier l'identité de la personne, l'authenticité du visa et la régularité du séjour en France ; - Faciliter l'identification des personnes étrangères en situation dite irrégulière en vue de leur éloignement ; - Faciliter la détermination et la vérification de l'identité d'une personne étrangère qui se déclare mineure privée temporairement ou définitivement de la protection de sa famille ; - Pour les personnes sollicitant une prise en charge au titre de l'aide médicale d'État : permettre aux organismes de sécurité sociale de vérifier la situation au regard du droit au séjour. (Article R. 142-1 du CESEDA)
Objectifs implicites	- Contrôler de manière stricte les personnes demandeuses de visa par le biais de l'utilisation des données biométriques. - Limiter l'octroi de titres de séjour pour les personnes étrangères.
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 entrées sur la plateforme France-Visas, lors de la demande et de la délivrance d'un visa, listées à l'annexe 2 de l'article R. 142-2 du CESEDA, soit : - **Les données relatives à la demande de visa dont les données générales** (information visa demandé ; numéro de la demande ; lien demande précédente ; nom de l'autorité saisie ; localisation de l'autorité saisie ; indication que l'autorité a été saisie en remplacement d'un autre État membre ; lieu et date de la demande ; type de visa ; motif du voyage ; nom, prénom et adresse de la personne invitante ; nom et adresse de la société ou compagnie invitante (personne morale) ; nom et prénom de la personne à contacter dans la société ou la compagnie invitante ; destination principale ; durée prévue du séjour ; date d'arrivée prévue ; date de départ prévue ; frontière de première entrée prévue ; route de transit prévue ; motif et date du retrait de la demande par le demandeur) - **Les données relatives à un groupe de demandeurs de visa** (type de groupe ; lien demande du groupe) - **Les données relatives à la personne demandeuse de visa soit les données d'état civil** (nom ; nom de naissance ; noms antérieurs ; prénoms ; sexe ; date de naissance ; lieu de naissance ; pays de naissance ; nationalité actuelle ; nationalité de naissance) - **Les données relatives aux documents de voyage** (type de document ; numéro du document ; autorité de délivrance ; date de délivrance ; date d'expiration), les données biométriques* (photographies ; empreintes digitales du demandeur) - **Les autres données** (résidence ; nom et prénom du père et de la mère du demandeur ; nom et coordonnées de l'employeur ; nom de l'établissement scolaire ou universitaire - si étudiant - ; profession actuelle et les données relatives au visa lui-même) - **Les données relatives au visa délivré** (information visa délivré ; lieu de la décision et date de délivrance du visa ; nom et localisation de l'autorité ayant délivré le visa ; indication que l'autorité a été saisie pour le compte d'un autre Etat membre ; validité territoriale dans laquelle le porteur du visa est autorisé à circuler ; type de visa délivré ; numéro de la vignette visa délivrée ; date de début et de fin de validité du visa ; nombre d'entrées autorisées ; durée de validité du visa ; durée du séjour autorisé ; information visa délivré sur feuillet séparé) - **Les données relatives à l'abandon d'examen de la demande** (information indiquant que l'examen de la demande de visa a été interrompu ; État membre compétent pour examiner la demande ; nom et localisation de l'autorité ayant interrompu l'examen de la demande ; date et lieu de l'interruption) - **Les données relatives au refus de visa** (information visa refusé ; nom et localisation de l'autorité qui a refusé le visa ; date, lieu et motif du refus) - Les données relatives à l'annulation, au retrait ou à la réduction de la durée de validité du visa (information visa annulé, retiré ou réduit dans sa validité ; nom et localisation de l'autorité ayant pris la décision ; date et lieu de la décision ; nouvelle date d'expiration de la validité du visa ; numéro de la nouvelle vignette ; motifs de la décision d'annulation, de retrait ou de réduction de validité de la vignette) - **Les données relatives à la prolongation du visa** (information visa prorogé ; nom et localisation de l'autorité ayant prorogé le visa ; date et lieu de la décision ; date de début et de fin de la période prorogée ; numéro de la nouvelle vignette ; période de prorogation de la durée du séjour, territoire sur lequel le porteur du visa est autorisé à circuler ; type de visa prorogé ; motifs de la prorogation) - **Les données recueillies ultérieurement lors des entrées et sorties de la personne en possession du visa** (date de première entrée, date de dernière entrée et date de sortie) (Article R. 142-2 du CESEDA)
Critères d'inscription dans ce fichier	Personne ayant déposé une demande de visa
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 données sont collectées par : - Les services chargés du contrôle aux frontières ; - Les services préfectoraux lorsqu'ils sont conduits à instruire des demandes de visa ; - Les chancelleries consulaires et les consulats des autres États membres de l'UE ; - Des prestataires agréés par les autorités chargées de la délivrance des visas et sous la responsabilité de ces dernières. Cela signifie que des entreprises privées peuvent collecter les données. (Articles R. 142-2 et R. 142-3 du CESEDA) Ont accès à ce fichier : - Le personnel du ministère de l'Europe et des affaires étrangères et du ministère chargé de l'immigration participant à l'instruction des demandes de visas individuellement désigné et spécialement habilité par le ministre dont il relève ; - Le personnel des préfectures individuellement désigné et spécialement habilité par le préfet ;

	- Le personnel chargé de l'application de la réglementation relative à la délivrance des titres de séjour, au traitement des demandes d'asile et à la préparation et à la mise en œuvre des mesures d'éloignement, individuellement désigné et spécialement habilité par le préfet ; - Le personnel des organismes de sécurité sociale désigné par la direction de ces organismes, pour les données relatives au nom, au prénom, à la date et au pays de naissance, à la photographie de la personne étrangère ainsi qu'à la délivrance d'un visa, à sa date, à sa durée de validité et aux documents de voyage ; - Le personnel des services de la police nationale et des unités de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme, individuellement désigné et spécialement habilité par la direction dont il relève ; - Le personnel des services spécialisés du renseignement individuellement désigné et spécialement habilité par la direction dont il relève, à des fins de « prévention des atteintes aux intérêts fondamentaux de la nation et des actes de terrorisme ». Peuvent être destinataires* des informations enregistrées dans VISABIO : - Le personnel chargé du contrôle aux frontières de la police et de la gendarmerie nationales et des douanes individuellement désigné et spécialement habilité ; - Le personnel du ministère de l'intérieur chargé de l'éloignement des personnes étrangères, individuellement désigné et spécialement habilité ; - Le personnel de police judiciaire des services de la police et de la gendarmerie nationale, individuellement désigné et spécialement habilité ; - Le personnel de police judiciaire relevant de la direction nationale de la police judiciaire, de la direction nationale de la police aux frontières ou de la direction générale de la gendarmerie nationale, pour des missions de vérification d'identité ; - Le personnel des douanes, individuellement désigné et spécialement habilité ; - Le personnel de l'Ofii chargé des procédures d'admission au séjour, individuellement désigné et spécialement habilité ; - Le personnel de la mise en œuvre de la protection de l'enfance, individuellement désigné et spécialement habilité par la présidence du conseil départemental ; - Le personnel de police judiciaire des services de la police et de la gendarmerie nationale, individuellement désigné et spécialement habilité, pour des missions de contrôle de l'authenticité des visas. (Articles R. 142-4, R. 142-5 et R. 142-6 du CESEDA)
Durée de conservation des données	5 ans à compter de l'enregistrement de la demande de visa. (Article R. 142-7 du CESEDA)
Échanges de données ?	VISABIO est le système français de suivi des demandes de visa qui est connecté au système européen d'information sur les visas (VIS). Il permet l'échange d'informations entre les autorités des Etats Schengen au travers du VIS. (Article R. 142-1 du CESEDA) Une communication automatique de données à caractère personnel renseignées dans le traitement France-Visas est prévue. Les données communiquées sont listées à l'annexe 2 du CESEDA et détaillées ci-dessus dans la partie « contenu des données ». Une interconnexion avec le fichier FAED est également envisagée (Next, 2022).
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'information, d'accès, de rectification et à la limitation s'exercent auprès : - De la direction des Français à l'étranger et de l'administration consulaire du ministère de l'Europe et des affaires étrangères ; - De la direction de l'immigration du ministère chargé de l'immigration ; - Ou du service où la demande de visa a été déposée. (Articles R. 142-8 et R. 142-9 du CESEDA)
Remarques	Avant la mise en place de VISABIO, un programme nommé « Biodev » a été expérimenté dans 5 consulats et 5 postes frontières. Dans une décision datant du 28 juin 2018, le Conseil d'État a jugé « que la consultation* du fichier VISABIO pouvait, à elle seule, permettre de remettre en cause l'authenticité des documents d'état civil produits par un jeune pris en charge par l'ASE » (Conseil d'État, 28 juin 2018, n° 403431 ; Gisti, Quadrature du Net, *Étrangers fichés*, Cahiers juridiques, 2022). Il est fréquent que le traitement VISABIO soit consulté par les services de police, et que les données enregistrées leur permettent de déterminer la qualité de majeur ou mineur d'une personne, influençant par conséquent la procédure suivie par celle-ci, et la protection qui lui est accordée. À plusieurs reprises, le Défenseur des droits a rappelé que les données contenues dans VISABIO ne peuvent de manière fiable indiquer l'âge d'une personne, notamment à cause des stratégies utilisées par les ressortissants de pays tiers afin d'obtenir des visas pour rejoindre la France, impliquant régulièrement l'utilisation de faux documents (Défenseur des droits, Décision n° 2020-051, 18 février 2020).

	Tous les 3 ans, le ministère chargé des affaires étrangères et le ministre chargé de l'immigration doivent effectuer une évaluation du traitement VISABIO et en tirer un rapport transmis à la Cnil. (Article R. 142-10 du CESEDA)
Textes qui régissent ce fichier	- Articles R. 142-1 à R. 142-10 du CESEDA - Décret n° 2020-1734 du 16 décembre 2020 portant partie réglementaire du CESEDA - Décret n° 2020-715 du 11 juin 2020 relatif à la consultation* du traitement de données* VISABIO aux fins de vérifier la situation des personnes sollicitant le bénéfice des prestations prévues aux articles L. 251-1 et L. 254-1 du code de l'action sociale et des familles - 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 - Loi n° 2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité - Règlement (CE) no 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) - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Sources	La Cimade, *Visa refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas*, Rapport d'observation, juillet 2010 Défenseur des droits, Décision n° 2020-051, 18 février 2020 Cnil, Délibération n° 2020-035 du 19 mars 2020 portant avis sur un projet de décret relatif au traitement de données* à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa (VISABIO) Gisti, La Quadrature du Net, « Étrangers fichés - Entrée, séjour, asile, éloignement, ordre public », octobre 2022 Manach Jean-Marc, « Le fichier des empreintes digitales sera interconnecté avec le casier judiciaire », Next, 3 juin 2022

Nom du fichier	**API-PNR**
Sens de l'acronyme	Advance passenger information - passenger name record / Renseignements préalables sur les voyageurs - Dossier passager
Date de création	26 septembre 2014
Quelle échelle ?	Européenne
Objectifs officiels	Chaque État membre de l'UE met en place ou désigne une autorité compétente qui sera chargée de la collecte des données PNR (Dossier passager), de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes. Elle sera également responsable de l'échange de ces données avec d'autres États membres. 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 surveillés.*** **»** (Cnil**, «** Le système API-PNR France », 2016) Les objectifs sont : - 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 dans le cas d'infractions et facilitation de la recherche des auteurs. La liste des infractions est établie à l'annexe II de la directive (UE) 2016/681 : Participation à une organisation criminelle, traite des êtres humains, fraude, aide à l'entrée et au séjour irréguliers, etc.
Objectifs implicites	Les données des passagers aériens sont traitées par les personnels affectés au sein de l'agence nationale des données de voyage afin de réaliser une évaluation des passagers aériens avant leur arrivée prévue sur le territoire national ou leur départ prévu de celui-ci et afin d'identifier les personnes pour lesquelles un examen plus approfondi est nécessaire au regard des finalités du traitement par les autorités. Pour Statewatch, « *la Directive sur les dossiers passagers (PNR) a introduit le premier système de profilage automatisé dans le régime de contrôle aux frontières de l'UE. Cela oblige presque toutes les compagnies aériennes à transmettre les données de toutes les personnes passagères des vols à destination, à l'intérieur ou à la sortie de l'UE à des « unités d'information passagers » gérées par les autorités nationales chargées de l'application de la loi. Les données sont comparées aux bases de données nationales et européennes et à des « critères prédéterminés » – une expression qui semble analogue à « indicateurs de risque » – afin de détecter les individus d'intérêt avant leur arrivée à un aéroport.* » (StateWatch, Automated Suspicion. The EU'S New travel surveillance initiatives, 2020)
Contenu des données	Les données API, dites d'enregistrement et d'embarquement, sont les informations : - Présentes dans les systèmes d'information d'enregistrement et d'embarquement des compagnies aériennes ou des plateformes aéroportuaires - Liées à l'enregistrement de la personne passagère provenant du passeport ou d'un autre document de voyage (nationalité, nom...) - Concernant le vol (date du vol, nombre total de personnes transportées...) Les données PNR, dites de réservation, sont les informations : - Fournies par les voyageurs et voyageuses au stade de la réservation commerciale et contenues dans les dossiers créés par les compagnies aériennes pour chaque vol ; - Qui 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.). De plus : - Une partie des données contenues dans le fichier des personnes recherchées FPR (une copie partielle et actualisée de ce dernier constituée des seuls signalements correspondant aux besoins exclusifs des missions confiées aux agents de l'agence nationale des données de voyage) ; - Pendant 24 heures : une copie partielle du FPR, du SIS, du FOVeS, le SILCF et le fichier des documents de voyage volés et perdus d'Interpol. (Liste exhaustive des données à l'article R. 232-14 du code de la sécurité intérieure)

Critères d'inscription dans ce fichier	Passager et passagère aérienne
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 Ce traitement est confié à l'agence nationale des données de voyage (ministère de l'intérieur).
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 selon l'article R. 232-15 du code de la sécurité intérieure les membres du personnel : - De la police nationale, de la direction générale de la sécurité intérieur et les militaires de la gendarmerie nationale, individuellement désignés, spécialement habilités et affectés au sein des services listés à l'article R. 232-15 ; - De la direction du renseignement et de la sécurité défense ; - De la direction du renseignement militaire ; - Des douanes affectés au sein des services listés à l'article R. 232-15 ; - Individuellement désigné et spécialement habilité par le directeur du service Tracfin ; - Individuellement désigné et spécialement habilité, affecté à la direction nationale du renseignement territorial et dans les services territoriaux de la police nationale chargés du renseignement territorial ; - Individuellement désigné et spécialement habilité par l'autorité hiérarchique dont il relève, affecté à la sous-direction de l'anticipation opérationnelle de la direction générale de la gendarmerie nationale ; - Individuellement désigné et spécialement habilité par l'autorité hiérarchique dont ils relèvent, affectés dans les services de la direction du renseignement de la préfecture de police ; - De la direction générale de la sécurité extérieure ; - De la direction générale de la sécurité intérieure ; - Des unités d'information passagers des États membres de l'Union européenne ; - D'Europol. Les destinataires* n'ont pas tous accès aux mêmes requêtes et aux mêmes modalités d'exploitation des données. Ainsi, une distinction est réalisée entre le personnel 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 5 ans à compter de leur réception dans le système, selon l'article 12 de la directive (UE) 2016/681. À l'expiration d'un délai de 6 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 ?	Interconnexion avec les fichiers FPR, SIS II, FOVeS, SILCF, SLTD.
Comment obtenir communication et rectification des données ?	Le droit d'opposition* ne s'applique pas. Les droits d'accès et de rectification se font directement auprès du Directeur de l'Agence nationale des données de voyage, Place Beauvau, 75800 PARIS CEDEX 08. Par exception, indirectement auprès de la Cnil : - Pour les mentions « connu » ou « inconnu » dans les autres fichiers (FPR, SIS II, FOVeS, SILCF, SLTD). - Pour les résultats des requêtes formulées par les unités et services. Lorsqu'une violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, l'agence nationale des données de voyage notifie cette violation à la personne concernée et à la Cnil.

Remarques	Comme le souligne la brochure, La folle volonté de tout contrôler (2024) : Le PNR actuel ne concerne que les voyages aériens. Cependant, depuis le mois de décembre 2019, le gouvernement affiche sa volonté d'étendre dans le futur le PNR aux voyages en train, bus et bateau. Les données sont comparées aux bases de données nationales et européennes et à des « critères prédéterminés ». Ces critères prédéterminés sont, selon l'article R. 232-13, « *définis en coopération avec les autorités mentionnées à l'article R. 232-15. Ils doivent être ciblés, proportionnés, spécifiques aux infractions et non discriminatoires. Ils ne peuvent être fondés sur des données à caractère personnel qui font apparaître, directement ou indirectement, la prétendue origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale ou celles qui sont relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle des personnes. Ils sont régulièrement mis à jour ou redéfinis* ». La liste des « critères prédéterminés » semblent ne pas avoir fait l'objet de publication. Enfin, si les entreprises de transports aériens refusent de transmettre les informations, la directive 2016/681 prévoit la mise en place d'un régime de sanction : « *Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. En particulier, les États membres déterminent le régime des sanctions, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne transmettent pas de données comme le prévoit l'article 8, ou ne les transmettent pas dans le format requis.* *Les sanctions prévues doivent être effectives, proportionnées et dissuasives.* »
Textes qui régissent ce fichier	- Articles R. 232-12 à R. 232-22 du code de la sécurité intérieure - Délibération n° 2014-308 du 17 juillet 2014 de la Cnil 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 intérieure - Délibération n° 2015-230 du 9 juillet 2015 de la Cnil 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 - Décret n° 2022-751 du 29 avril 2022 portant dispositions réglementaires relatives à l'agence nationale des données de voyage - Décret n° 2018-714 du 3 août 2018 relatif au « système API-PNR France » et modifiant le code de la sécurité intérieure (partie réglementaire) - 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 - 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 - 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 - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 Cnil, « Le système API-PNR France », août 2016 Statewatch, « Automated Suspicion. The EU'S New travel surveillance initiatives », juillet 2020

Nom du fichier	**CIR**
Sens de l'acronyme	Common identity repository / Répertoire commun de données d'identité
Date de création	Les deux règlements régissant le CIR ont été publiés au Journal officiel de l'Union européenne le 22 mai 2019. Celui-ci n'est toutefois pas encore opérationnel à l'heure de la publication de ce document. Les systèmes sont censés être opérationnels d'ici 2027. (Voir les conditions pour que le CIR devienne opérationnel à l'article 72 paragraphe 3 du règlement (UE) 2019/817)
Quelle échelle ?	Européenne
Objectifs officiels	Le traitement CIR vise à stocker les données d'identité, biométriques* et relatives aux documents de voyage renseignées dans les traitements EES, VIS, ETIAS, Eurodac, et ECRIS-TCN, afin que celles-ci soient centralisées plutôt que stockées au sein de chacun de ces fichiers. Ainsi, les objectifs du CIR sont : - Participer à l'interopérabilité* des systèmes d'information de l'Union européenne (EES, ETIAS, VIS, Eurodac, SIS, ECRIS-TCN) ;

	- Faciliter l'identification des personnes enregistrées dans les systèmes EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN afin de « *faciliter les contrôles d'identité pour les [personnes voyageant] de bonne foi et de lutter contre la fraude à l'identité* » ; - Stocker les données relatives à l'identité, aux documents de voyage et les données biométriques* des personnes inscrites dans les systèmes d'information de l'Union européenne, les comparer et les mettre en correspondance de manière automatique pour une identification plus précise des personnes ; - « *Le CIR devrait donc faciliter et rationaliser l'accès des autorités chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière, aux systèmes d'information de l'UE qui qui ne sont pas exclusivement créés à des fins de prévention ou de détection des infractions graves, ou d'enquêtes en la matière*. » (Paragraphe 25 du préambule du règlement (UE) 2019/817)
Objectif implicite	Permettre une surveillance accrue des personnes étrangères à l'entrée et sur le territoire de l'UE
Contenu des données	- Les données renseignées par les autorités frontalières créant un dossier EES pour une personne ressortissante d'un pays dit tiers se présentant au point de contrôle frontalier, notamment relatives à l'identité de la personne voyageuse, le type et numéro de ses documents de voyage, le pays de délivrance et la date d'expiration de ces documents, l'image faciale de la personne et les données dactyloscopiques* enregistrées le cas échéant (16, paragraphe 1, points a) à d), 17 paragraphe 1, points a), b) et c) et 18 paragraphes 1 et 2 du règlement (UE) 2017/2226) ; - Certaines données extraites du traitement VIS relatives à l'identité, à la ou aux nationalités de la personne concernée, le type et numéro du document de voyage, l'autorité l'ayant délivré et la date de délivrance et d'expiration, la photographie de la personne demandeuse de visa, et ses empreintes digitales (Article 9, point 4) a) à c), et points 5) et 6), du règlement (CE) n° 767/2008) ; Les données extraites du traitement ETIAS relatives à l'identité de la personne demandeuse d'une autorisation de voyage et de ses parents, sa ou ses nationalités, le type, numéro et pays de délivrance de son document de voyage, ainsi que les dates de délivrance et d'expiration de ce document (Article 17, paragraphe 2, points a) à e), du règlement (UE) 2018/1240). (Article 18 du règlement (UE) 2019/817)
Critères d'inscription dans ce fichier	Personne inscrite dans le système EES, VIS, ETIAS, Eurodac, SIS et/ou ECRIS-TCN. Lors de l'enregistrement de données personnelles dans l'un de ces fichiers, un dossier individuel est créé dans le CIR, stockant les informations sur l'identité de la personne.
Autorité(s) compétente(s)	L'EU-Lisa est chargée de développer le CIR et d'en assurer la gestion technique (Article 17 du règlement (UE) 2019/817). Les autorités des États membres responsables du traitement pour l'EES, le VIS et l'ETIAS sont responsables du traitement de ces données dans le CIR (Article 40 Règlement (UE) 2019/817).
Qui a accès à ce fichier ?	Ont accès au CIR : - Les services de police habilités par les mesures législatives nationales, à des fins d'identification d'une personne âgée de plus de 12 ans, ou de vérification de l'authenticité d'un document de voyage fourni par une personne. L'interrogation du CIR peut se faire à l'aide des données biométriques* de la personne relevées lors d'un contrôle d'identité, si les mesures législatives nationales le permettent (Article 20 du règlement (UE) 2019/817). - Les autorités chargées de la vérification manuelle des identités multiples au sein des systèmes d'information de l'Union européenne selon le fichier avec lequel une correspondance est identifiée avec le CIR, conformément à l'article 29 du règlement (UE) 2019/817) (Article 21 du règlement (UE) 2019/817). Peuvent consulter le CIR : - Les autorités désignées pour la prévention ou la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière et Europol peuvent consulter le CIR « *pour savoir si des données sur une personne en particulier figurent dans l'EES, le VIS ou ETIAS* » (Article 22 du règlement (UE) 2019/817). Les données stockées dans le CIR ne peuvent faire l'objet d'un transfert vers un pays dit tiers, une organisation internationale ou une entité privée, ni être mises à leur disposition, sauf pour les exceptions qui sont mentionnées dans les règlements régissant chacun des systèmes d'information lié au CIR (Article 50 du règlement (UE) 2019/817).
Durée de conservation des données	Les données contenues dans le CIR sont conservées « aussi longtemps que les données correspondantes sont stockées dans au moins un des systèmes d'information de l'UE dont les données figurent dans le CIR. La création d'un lien n'a aucune incidence sur la période de conservation de chaque élément des données liées. » (Article 23 du règlement (UE) 2019/817)
Échanges de données	Le CIR est un outil permettant l'interopérabilité* des systèmes d'information de l'Union européenne, soit EES, le VIS, ETIAS, EURODAC, le SIS II et l'ECRIS-TCN. Il est qualifié d'« élément d'interopérabilité* » et permet la comparaison et la mise en correspondance des données stockées dans ces différents traitements. Le CIR « *devrait prévoir un réservoir partagé pour les données d'identité, les données du document de voyage et les données biométriques* des personnes enregistrées dans l'EES, le VIS, ETIAS, Eurodac et l'ECRIS-TCN* » (Paragraphe 26 du préambule du règlement (UE) 2019/817). Pour ce faire, un dossier individuel est créé pour chaque personne enregistrée dans l'EES, le VIS, ETIAS, Eurodac, le SIS et/ou l'ECRIS-TCN (Article 17 du règlement (UE) 2019/817).

	Le CIR peut être interrogé via le portail de recherche européen (ESP)[29] (Paragraphe 17 du préambule du règlement (UE) 2019/817). L'ESP comprend une infrastructure de communication sécurisée avec l'EES, le VIS, l'ETIAS, Eurodac, le SIS central, l'ECRIS-TCN, les données Europol et les bases de données d'Interpol, ainsi qu'avec les infrastructures centrales du CIR et du détecteur d'identités multiples (MID), également créé par le règlement (UE) 2019/817 (Article 6 du règlement (UE) 2019/817). Les autorités des États membres et agences de l'Union ayant accès à au moins l'un des systèmes d'information de l'UE peuvent utiliser l'ESP (Article 7 du règlement (UE) 2019/817). Ces autorités peuvent lancer une requête en soumettant les données alphanumériques* ou biométriques* à l'ESP. « Lorsqu'une requête a été lancée, l'ESP interroge l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN et le CIR ainsi que les données d'Europol et les bases de données d'Interpol, simultanément, à l'aide des données envoyées par l'utilisateur et conformément au profil d'utilisateur. » Aucune information concernant des données à laquelle l'autorité lançant la requête n'a pas accès en vertu du droit de l'Union ne peut être communiquée par l'ESP (Article 9 du règlement (UE) 2019/817). **Le service partagé d'établissement de correspondances biométriques* (BMS)** [30], également créé par le règlement (UE) 2019/817, doit être utilisé avec l'ESP afin de comparer les données enregistrées dans le CIR et dans le SIS de manière automatique. Dans l'autre sens, le CIR et le SIS devraient être en mesure d'utiliser le BMS afin de détecter les liens possibles sur la base des données biométriques, et l'ESP pour les liens possibles sur la base des données alphanumériques*. Le CIR et le SIS devraient également pouvoir détecter les données identiques ou similaires relatives à une personne stockées dans plusieurs systèmes (Paragraphe 41 du préambule du règlement (UE) 2019/817). La vérification des différentes identités doit se faire manuellement par l'autorité nationale ou l'agence de l'Union qui a enregistré les données dans le système concerné. Pour ce faire, l'autorité en question devrait pouvoir avoir accès aux données stockées dans le CIR, le SIS et le MID (Paragraphe 42).
Comment obtenir communication et rectification des données ?	Il convient de mettre à disposition des personnes concernées un portail en ligne qui facilite l'exercice par celles-ci de leurs droits d'accès à leurs données à caractère personnel et de leurs droits de rectification, d'effacement et de limitation du traitement de ces données. La mise en place et la gestion dudit portail devraient incomber à l'EU-Lisa (Paragraphe 73 du préambule du règlement (UE) 2019/817).
Remarques	En parallèle du CIR, d'autres éléments permettant l'interopérabilité* des systèmes d'information de l'Union sont créés : un portail de recherche européen, un service partagé d'établissement de correspondances biométriques* et un détecteur d'identités multiples[31]. Le contrôleur européen de la protection des données a rendu un avis en 2018 sur les deux règlements établissant le cadre de l'interopérabilité* des systèmes d'information de l'Union. Il souligne « les risques d'abus » à la mise en place d'une base de données centralisées et les risques de « *nuire gravement à un nombre potentiellement élevé de personnes* ». Il précise que les données stockées dans le CIR, de nature très sensible, vont concerner des millions de personnes. Le contrôleur insiste également sur le fait que les données contenues dans le CIR peuvent être communiquées aux autorités de police des États membres à des fins de « *prévention et de la lutte contre la migration irrégulière et/ou contribuer à un niveau élevé de sécurité* », ce qui constitue un objectif très large et pas défini de manière suffisamment précise pour éviter les dérives. (European data protection supervisor, Opinion 4/218 on the proposals for two regulations, 2018)
Textes qui régissent 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) - Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 - Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 - Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité* des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil - Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité* des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 - Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'« Eurodac » pour la comparaison des données biométriques* aux fins de l'application efficace des règlements (UE) 2024/1351 et (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de

[29] ESP est un portail de recherche européen qui permet aux personnels des États membres ayant accès à l'ESP de consulter systématiquement les bases de données de l'UE, d'Europol et d'Interpol (Pour plus d'informations, voir le règlement (UE) 2019/817).
[30] BMS est le service partagé d'établissement de correspondances biométriques. Il permet d'effectuer des recherches à partir des données biométriques* du CIR et du SIS dans les autres bases de données de l'UE.
[31] Ces outils ne sont pas développés dans la présente boîte à fichiers car elle s'est cantonnée à l'analyse des fichiers.

	l'identification des ressortissants de pays tiers et 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, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil
Sources	Direction générale des politiques internes, Département thématique des droits des citoyens et des affaires constitutionnelles, « Interopérabilité des systèmes d'information européens dans le domaine de la justice et des affaires intérieures », étude demandée par la commission LIBE, Synthèse, avril 2018 EUR-Lex, « Interopérabilité des systèmes d'information de l'Union européenne dans le domaine de la liberté, de la sécurité et de la justice », 2024 European Data Protection Supervisor, « Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems », avril 2018 Statewatch, « The "point of no return" - Interoperability morphs into the creation of a Big Brother centralised EU state database including all existing and future Justice and Home Affairs databases », mai 2018

Nom du fichier	**ECRIS-TCN**
Sens de l'acronyme	European criminal records information system - Third country nationals / Système européen d'informations sur les casier judiciaires – ressortissants de pays tiers ECRIS-TCN est composé : - D'un système central ; - Du répertoire commun de données d'identité (CIR) ; - Un point d'accès central national dans chaque État membre ; - Un logiciel* d'interface permettant aux autorités de se connecter au système central ; - Une infrastructure de communication entre le système central et les points d'accès centraux nationaux ; - Une infrastructure de communication entre le système central et les infrastructures centrales de l'ESP[32] et du CIR. ECRIS-TCN remplace l'ECRIS.
Date de création	17 avril 2019 Avec pour objectif qu'il soit opérationnel d'ici 2027 (Statewatch, « Retards dans les bases de données : nouveau calendrier pour l'interopérabilité des systèmes de police et de migration de l'UE d'ici 2027 », 2023)
Quelle échelle ?	Européenne
L'ancien fichier ECRIS	ECRIS est opérationnel depuis avril 2012. Il « *permet un échange électronique d'informations sur les casiers judiciaires sur une base décentralisée entre les États membres. Il permet aux autorités chargées du casier judiciaire des États membres d'obtenir des informations complètes sur les condamnations antérieures des personnes ressortissantes de l'UE auprès de l'État membre dont ils ont la nationalité*. » (EUR-Lex, Système européen d'information sur les casiers judiciaires (ECRIS), 2009)
Objectifs officiels	ECRIS-TCN est « *un système permettant d'identifier les États membres de l'Union européenne (UE) qui détiennent des informations sur les condamnations antérieures de personnes ressortissantes de « pays tiers » et d'apatrides* ». Le fichier ECRIS TCN permet de : - Soutenir l'objectif d'ETIAS consistant à contribuer à un niveau élevé de sécurité en permettant une évaluation approfondie des risques que les demandeurs et demandeuses présentent en matière de sécurité, avant leur arrivée aux points de passage des frontières extérieures, en vue de déterminer s'il existe des indices concrets ou des motifs raisonnables permettant de conclure que la présence de la personne sur le territoire des États membres présente un risque en matière de sécurité ; - Soutenir l'objectif du VIS consistant à déterminer si le demandeur ou la demandeuse d'un visa, d'un visa de long séjour ou d'un titre de séjour pourrait constituer une menace pour l'ordre public ou la sécurité intérieure, conformément au règlement (CE) 767/2008 ; - Faciliter l'identification correcte des personnes et aide à cette identification ; - Utiliser des données à des fins d'établissement de rapports et de statistiques (Article 32). (Article 1 du règlement (UE) 2019/816) C'est l'État membre responsable de la condamnation qui crée la fiche de la personne, après l'inscription de la condamnation dans le casier judiciaire.
Objectifs implicites	Un des objectifs implicites d'ECRIS-TCN est de faciliter la coopération policière et l'échange d'informations numériques concernant les personnes étrangères.

[32] ESP est un portail de recherche européen qui permet aux personnels des États membres ayant accès à l'ESP de consulter systématiquement les bases de données de l'UE, d'Europol et d'Interpol (Pour plus d'information voir le règlement (UE) 2019/817).

	En regroupant les données uniquement des personnes ressortissantes de pays dits tiers et condamnées dans une base de données, ECRIS-TCN contribue **à une forme de double peine** et à spécifier la condition de personnes étrangères en France. Et ce, notamment car l'ECRIS-TCN peut être consulté dans le cadre des procédures de visas, d'acquisition de la citoyenneté et de migration, y compris pour les procédures d'asile. Alors que cette base de données est censée avoir été créée à des fins de lutte contre le terrorisme et la criminalité grave.
Contenu des données	Le fichier ECRIS-TCN contient : - Des données alphanumériques* - Nom, prénoms, date de naissance, lieu de naissance, la/les nationalité(s), genre, noms précédents, le code de l'État membre de condamnation - Les informations à inclure lorsqu'elles ont été inscrites dans le casier judiciaire : les noms des parents - Les informations à inclure si l'autorité centrale en dispose : le numéro d'identité ou le type et le numéro des documents d'identité de la personne concernée (y compris les documents de voyage, ainsi que le nom de l'autorité les ayant délivrés), les pseudonymes ou noms d'emprunt - Des images faciales du ressortissant d'un pays tiers condamné, si le droit de l'État membre de condamnation autorise la collecte et la conservation des images faciales des personnes condamnées. La Commission européenne est habilitée à utiliser la reconnaissance faciale selon les critères de nécessité et de proportionnalité. (Article 5 du règlement (UE) 2019/816) De plus, en France, les empreintes digitales de chaque doigt recueilli à l'occasion de procédures pénales et dans le cadre d'un délit puni d'une peine d'emprisonnement sont transmis au fichier ECRIS-TCN. (Article 771-2 du code de procédure pénale)
Critères d'inscription dans ce fichier	Toute personne ressortissante de pays hors UE qui a fait l'objet de condamnations dans les États membres de l'UE : - Condamné à une peine privative de liberté d'au moins 6 mois ; - Condamné pour avoir commis une infraction pénale punissable, en vertu du droit de l'État membre, d'une peine privative de liberté d'une durée maximale d'au moins 12 mois ; Au cours des 25 dernières années pour une infraction terroriste ou au cours des 15 dernières années pour toute autre infraction pénale.
Autorité(s) compétente(s)	L'agence EU-Lisa est responsable du fichier ECRIS-TCN. Chaque État membre est responsable de : - L'établissement d'une connexion sécurisée entre son casier judiciaire national, ses bases de données dactyloscopiques* et son point d'accès central national ; - Le développement, le fonctionnement et la maintenance de cette connexion ; - L'établissement d'une connexion entre ses systèmes nationaux et l'application de référence de l'ECRIS-TCN ; - La gestion et des modalités de l'accès à l'ECRIS-TCN. (Article 12 du règlement (UE) 2019/816)
Qui a accès à ce fichier ?	Les autorités centrales des États membre de l'UE ont accès au fichier ECRIS-TCN pour : - Les procédures de visas, d'acquisition de la citoyenneté et de migration, y compris les procédures d'asile ; - La vérification par une personne de son propre casier judiciaire, à sa demande ; - L'habilitation de sécurité ; - L'obtention d'une licence ou d'un permis ; - Les enquêtes menées dans le cadre d'un recrutement professionnel ; - Les enquêtes menées dans le cadre d'un recrutement en vue d'activités bénévoles impliquant des contacts directs et réguliers avec des enfants ou des personnes vulnérables ; - Les vérifications en rapport avec des marchés publics et des concours publics. Tout État membre qui décide, si le droit national le prévoit et conformément à celui-ci, d'utiliser l'ECRIS-TCN à des fins autres pour obtenir des informations sur les condamnations antérieures, notifie à la Commission ou à tout moment par la suite, ces autres fins et toutes les modifications qui y sont apportées. La Commission européenne publie ces notifications au Journal officiel de l'Union européenne dans les trente jours suivant leur réception. Chaque État membre notifie à l'EU-Lisa le nom de son ou de ses autorités centrales qui bénéficient d'un accès pour inscrire, rectifier, effacer ou consulter des données ou effectuer des recherches dans celles-ci, ainsi que toute modification à cet égard. (Article 34 du règlement (UE) 2019/816) Les autorités compétentes peuvent également interroger l'ECRIS-TCN en utilisant des images faciales. Elles doivent cependant le notifier à la Commission qui délivrera ou non une habilitation. (Article 7 du règlement (UE) 2019/816) - Le personnel dûment autorisé de l'EU-Lisa, des autorités compétentes et de la Commission ont accès aux données traitées dans l'ECRIS-TCN à des fins statistiques et d'établissement de rapports ne permettant aucune identification d'individus. (Article 32 du règlement (UE) 2019/816)

	- Le personnel autorisé d'Eurojust, d'Europol et du Parquet européen dans le cadre de leur responsabilité dans la gestion et les modalités d'accès d'ECRIS-TCN Peuvent consulter le fichier, sans inscrire, rectifier ou effacer des données inscrites dans l'ECRIS-TCN : - Les agences européennes : Eurojust, Europol et le Parquet européen ; - Les pays tiers et les organisations internationales peuvent, dans le cadre d'une procédure pénale, adresser des demandes d'information, le cas échéant, sur l'État membre détenant des informations sur le casier judiciaire d'une personne ressortissante d'un pays tiers à Eurojust.
Durée de conservation des données	- Chaque fichier de données est conservé dans le système central et dans le CIR tant que les données relatives aux condamnations de la personne concernée sont conservées dans le casier judiciaire ; - Ou 25 ans après la création de la mention en ce qui concerne les condamnations liées à des infractions terroristes ; - Ou 15 ans après la création de la mention en ce qui concerne les condamnations liées à d'autres infractions pénales, la date la plus proche étant retenue.
Échanges de données	Interconnexion avec VIS, ETIAS. Échange de données avec le FAED, le CIR et les données auxquelles ces fichiers ont accès (voir CIR « échanges de données »).
Comment obtenir communication et rectification des données ?	Les demandes des personnes ressortissantes de pays dits tiers concernant les droits d'accès aux données à caractère personnel, de rectification et d'effacement de ces données et de la limitation de leur traitement, peuvent être adressées à l'autorité centrale de tout État membre[33]. - Les États membres peuvent modifier ou effacer les données qu'ils ont inscrites dans le système central et dans le CIR. - Toute modification des informations figurant dans le casier judiciaire qui ont conduit à la création d'un fichier de données doivent être modifiées à l'identique dans le fichier ECRIS-TCN. - Les États membres peuvent également lancer une procédure de vérification des données ou de la licéité de leur traitement. Toute personne a le droit d'introduire une réclamation et le droit de former un recours dans l'État membre de condamnation qui lui a refusé le droit d'accès aux données la concernant ou le droit d'en obtenir la rectification ou l'effacement visés à l'article 25, conformément au droit national ou de l'Union. Dans le cadre des données contenues dans le fichier ECRIS-TCN, c'est l'État membre qui a inscrit ces données qui est responsable de dommage subi ou l'EU-Lisa concernant la sécurité des données contenues dans le fichier. Cependant, l'État membre qui est responsable du dommage subi ou l'EU-Lisa, respectivement, est exonéré partiellement ou totalement de sa responsabilité s'il prouve que le fait générateur du dommage ne lui est pas imputable. (Article 20 du règlement (UE) 2019/816) En France, la personne peut faire une demande au service du casier judiciaire national. Si une personne ressortissante française a été condamnée par une juridiction étrangère et que cette condamnation figure au bulletin n° 1 de son casier judiciaire, il ou elle peut demander le retrait de cette mention au tribunal correctionnel de son domicile, ou de Paris s'il réside à l'étranger (Article 770-1 du code de procédure pénal).
Textes qui régissent ce fichier	- Décision-cadre 2009/315/JA I informations sur ces condamnations antérieures au moyen du système européen d'information sur les casiers judiciaires (ECRIS) - Loi du 22 décembre 2021 pour la confiance dans l'institution judiciaire - Ordonnance n° 2022-1524 du 7 décembre 2022 relative au casier judiciaire national automatisé prise pour l'application du règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 et de la directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 - Règlement (UE) 2019/816 du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN) - Règlement (UE) 2024/1352 du 14 mai 2024 modifiant les règlements (UE) 2019/816 et (UE) 2019/818 aux fins de l'introduction du filtrage des ressortissants de pays tiers aux frontières extérieures
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » EUR-Lex, Système européen d'information sur les casiers judiciaires (ECRIS), 2009 Statewatch, *Retards dans les bases de données : nouveau calendrier pour l'interopérabilité des systèmes de police et de migration de l'UE d'ici 2027*, 2023 Statewatch, *Frontex and interoperable databases: knowledge as power?*, 2023 Statewatch, *UE : Suivi du pacte : Accès aux casiers judiciaires pour le « filtrage » des migrants*, 2022

[33] Au moment de la publication de la boîte à fichiers, les informations sur quelle sera l'autorité centrale n'était pas disponible.

Nom du fichier	**EES**
Sens de l'acronyme	Entry-exit system / Système d'entrée-sortie
Date de création	Le règlement (UE) 2017/2226 a été publié au Journal officiel de l'Union européenne le 9 décembre 2017. La mise en œuvre de l'EES était initialement prévue pour 2022. Toutefois, des contraintes techniques ont mené à de nombreux reports successifs et le démarrage des opérations du système est, à ce jour, prévu pour octobre 2025.
Quelle échelle ?	Européenne
Objectifs officiels	Contrôler et enregistrer électroniquement les entrées, les sorties et les refus d'entrée dans l'espace Schengen des ressortissants de pays non-membres de l'UE franchissant les frontières extérieures, ainsi que les durées de leur séjour. Le système EES vise à remplacer l'obligation de tamponner les passeports des personnes ressortissantes de pays dits tiers. Il s'applique aux personnes soumises à visa mais également à celles qui sont exemptées de visas. Le système EES est également mis en place dans des objectifs de : - Moderniser de la gestion des frontières extérieures de l'UE ; - Lutter contre l'usurpation d'identité ; - Faciliter l'identification des personnes dépassant la durée autorisée de leur séjour au sein de l'espace Schengen ; - Renforcer des contrôles aux frontières extérieures de l'UE ; - Améliorer le partage d'informations en temps réel entre les autorités frontalières de l'UE. (Site de l'UE, Qu'est-ce que l'EES ?, 2025)
Objectif implicite	Restreindre et contrôler davantage le nombre de personnes étrangères entrant sur le territoire de l'Union européenne.
Contenu des données	Pour les personnes ressortissantes de pays dits tiers soumises à l'obligation de visa : - Nom, prénom(s), date de naissance, nationalité(s), sexe - Type et numéro du ou des documents de voyage, la date d'expiration de leur validité et pays de délivrance - Image faciale Pour chaque entrée sur le territoire Schengen : - Date et heure de l'entrée - Point de passage frontalier de l'entrée et autorité ayant autorisé l'entrée - Statut du ressortissant (membre de la famille d'un citoyen de l'UE, ressortissant de pays tiers jouissant d'un droit à la libre circulation, non titulaire d'une carte ou d'un titre de séjour) - Numéro de la vignette du visa de court séjour, pays de délivrance du visa, type de visa, date de fin de la durée maximale du séjour autorisé mise à jour à chaque entrée, date d'expiration de la validité du visa - À la première entrée : nombre d'entrée autorisées et durée du séjour autorisé par le visa - Potentielle limitation de la validité territoriale du visa Pour chaque sortie du territoire Schengen : - Date et heure de la sortie - Point de passage frontalier de sortie Par ailleurs, « *immédiatement après la date d'expiration du séjour autorisé, la fiche d'entrée/de sortie est assortie d'un drapeau par l'EES* ». Le drapeau est un pictogramme visuel permettant d'identifier les visas expirés et de faire savoir à l'agent/l'agente consultant l'EES que les données de la personne peuvent être consultées sur la liste. En effet, les données de la personne n'ayant pas quitté le territoire Schengen avant l'expiration de son visa sont inscrites sur une liste mise à disposition d'autorités nationales désignées par les États membres. Ces autorités désignées peuvent introduire, modifier, effacer et consulter ces données, notamment à des fins répressives. Enfin, il est indiqué dans la fiche d'une personne si elle bénéficie du programme national d'allègement des formalités d'un État membre conformément à l'article 8 quinquies du règlement (UE) 2016/399. (Article 16 du règlement (UE) 2017/2226) Pour les personnes ressortissantes de pays tiers exemptées de l'obligation de visa : - Nom, prénom(s), date de naissance, nationalité(s), sexe - Type et numéro du ou des documents de voyage, la date d'expiration de leur validité et pays de délivrance

	- Image faciale - Données dactyloscopiques* de la main droite ou, à défaut, de la main gauche, pour l'établissement automatisé de correspondances biométriques - S'il y a lieu, notification de bénéficiaire d'un programme national d'allègement des formalités d'un État membre Pour chaque entrée sur le territoire Schengen : - Date et heure de l'entrée - Point de passage frontalier de l'entrée et autorité ayant autorisé l'entrée - Statut du ressortissant (membre de la famille d'un citoyen de l'UE, ressortissant de pays tiers jouissant d'un droit à la libre circulation, non titulaire d'une carte ou d'un titre de séjour) Pour chaque sortie du territoire Schengen : - Date et heure de la sortie - Point de passage frontalier de sortie « *[I]mmédiatement après la date d'expiration du séjour autorisé, la fiche d'entrée/de sortie est assortie d'un drapeau par l'EES* ». Les données de la personne n'ayant pas quitté le territoire Schengen avant l'expiration du séjour autorisé sont également inscrites sur la liste mise à disposition d'autorités nationales désignées par les États membres. - Les enfants de moins de 12 ans ainsi que les personnes dont il est physiquement impossible de relever les empreintes digitales sont exemptées de l'obligation de donner leurs empreintes digitales. Toutefois, il n'existe pas de limite d'âge pour la collection des images faciales. (Article 17 du règlement (UE) 2017/2226) Pour les personnes ressortissantes de pays tiers auxquelles l'entrée est refusée : - Si aucun dossier sur l'EES n'existait avant le refus d'entrée, l'autorité frontalière en crée un, incluant : - Pour les personnes ressortissantes de pays tiers soumises à l'obligation de visa : nom, prénom(s), date de naissance, nationalité(s), sexe, type et numéro du ou des documents de voyage, date d'expiration de leur validité et pays de délivrance, image faciale, potentielle notification de bénéficiaire d'un programme national d'allègement des formalités d'un État membre - Pour les personnes ressortissantes de pays tiers exemptées de l'obligation de visa : nom, prénom(s), date de naissance, nationalité(s), sexe, type et numéro du ou des documents de voyage, date d'expiration de leur validité et pays de délivrance, image faciale, données dactyloscopiques* de la main droite ou, à défaut, de la main gauche, pour l'établissement automatisé de correspondances biométriques, potentielle notification de bénéficiaire d'un programme national d'allègement des formalités d'un État membre - Si une personne ressortissante de pays dits tiers se voit refuser l'entrée pour possession de faux documents de voyage ou permis de séjour ou signalement dans des fichiers SIS ou nationaux, et qu'aucune donnée biométrique n'est enregistrée dans l'EES, un dossier est également créé par les autorités frontalières, incluant : nom, prénom(s), date de naissance, nationalité(s), sexe, type et numéro du ou des documents de voyage, date d'expiration de leur validité et pays de délivrance, image faciale et, pour les ressortissant·es de pays tiers exempté·es de l'obligation de visa, les données dactyloscopiques* de la main droite ou, à défaut, de la main gauche, pour l'établissement automatisé de correspondances biométriques*, potentielle notification de bénéficiaire d'un programme national d'allègement des formalités d'un État membre - Si une personne ressortissante de pays tiers se voit refuser l'entrée pour signalement dans des fichiers SIS ou nationaux et que ses données biométriques* sont enregistrées dans le signalement SIS**,** ces dernières ne sont pas introduites dans l'EES - Si une personne ressortissante de pays tiers se voit refuser l'entrée car elle est considérée comme représentant un danger pour l'ordre public, la sécurité intérieure, la santé publique ou les relations internationales d'un ou de plusieurs États membres de l'UE, en vertu de la partie B de l'annexe V du règlement (UE) 2016/399, et lorsque aucun dossier antérieur contenant des données biométriques* n'est enregistré dans l'EES pour cette personne, « *les données biométriques* ne sont introduites dans l'EES que si l'entrée est refusée parce que le ressortissant de pays tiers est considéré comme représentant un danger pour la sécurité intérieure, y compris, le cas échéant, pour certains aspects de l'ordre public* » - Si une personne ressortissante de pays tiers se voit refuser l'entrée pour refus de fournir ses données biométriques* – afin de créer son dossier individuel dans le système EES ou d'effectuer les vérifications aux frontières **–** en vertu de la partie B de l'annexe V du règlement (UE) 2016/399, les autorités frontalières créent un dossier dans l'EES sans y ajouter les données biométriques. Si cette personne est en possession d'un document de voyage électronique lisible par machine (DVLM-e), son image faciale est extraite de ce document Par ailleurs, pour tout refus d'entrée notifié à une personne ressortissante de pays tiers, les données suivantes sont inscrites dans le système EES : - La date et l'heure du refus d'entrée - Le point de passage frontalier

	- L'autorité qui a refusé l'entrée - Les raisons avancées pour le refus d'entrée, en vertu de la partie B de l'annexe V du règlement (UE) 2016/399 En ce qui concerne les personnes ressortissantes de pays tiers soumises à obligation de visa, sont également incluses : - Le numéro de la vignette visa de court séjour, et l'État membre de délivrance, le type de visa de court séjour, la date de fin de la durée maximale du séjour autorisé par le visa de court séjour, qui est mise à jour à chaque entrée, et la date d'expiration de la validité du visa de court séjour s'il y a lieu - À la première entrée sur la base d'un visa de court séjour, le nombre d'entrées autorisées et la durée du séjour autorisé par le visa de court séjour, comme indiqué sur la vignette visa de court séjour - S'il y a lieu, les informations indiquant que le visa de court séjour a été délivré avec une validité territoriale limitée - Pour les États membres qui n'appliquent pas encore l'acquis de Schengen dans son intégralité mais qui mettent en œuvre l'EES, une notification, s'il y a lieu, indiquant que le ressortissant de pays tiers a utilisé un visa de court séjour national pour l'entrée La fiche de refus d'entrée est rattachée au dossier individuel de la personne concernée dans le système EES. (Article 18 du règlement (UE) 2017/2226) Données à ajouter en cas de retrait, d'annulation ou de prorogation d'une autorisation de court séjour : Lorsque l'autorisation de court séjour d'une personne est retirée, annulée, prolongée ou prorogée, les données suivantes sont incluses dans sa fiche : - Informations relatives au retrait, à l'annulation, à la prolongation ou à la prorogation du visa ou de l'autorisation de court séjour - Identité de l'autorité ayant modifié l'autorisation ou le visa - Le lieu et la date de la décision - S'il y a lieu, le nouveau numéro de vignette visa, incluant le pays de délivrance - Le cas échéant, la période de prolongation de la durée du séjour autorisé - Le cas échéant, la nouvelle date d'expiration du séjour autorisé ou du visa Ces données peuvent être extraites du fichier VIS par les autorités chargées des visas ayant pris la décision d'annuler, de retirer ou de proroger un visa. Sont également inscrits les motifs de prolongation ou retrait ou d'annulation du court séjour, soit : - Une décision de retour adoptée en vertu de la directive 2008/115/CE du Parlement européen et du Conseil - Toute autre décision prise par les autorités compétentes de l'État membre, conformément au droit national, entraînant le retour, l'éloignement ou le départ volontaire d'un ressortissant de pays tiers qui ne remplit pas ou ne remplit plus les conditions d'entrée ou de séjour sur le territoire des États membres Enfin, le départ ou l'éloignement d'une personne à la suite d'une décision de retour ou de toute autre décision prise par les autorités compétentes d'un État membre, l'autorité compétente introduit les données dans la fiche EES de la personne concernée. (Article 19 du règlement (UE) 2017/2226) Données à ajouter en cas de renversement de la présomption concernant le non-respect par un ressortissant de pays tiers des conditions de durée du séjour autorisé : Lorsque aucun dossier individuel n'a été créé dans l'EES pour un ressortissant de pays tiers présent sur le territoire d'un État membre, ou en l'absence de dernière fiche pertinente d'entrée/de sortie pour une personne ressortissante de pays tiers, les autorités compétentes peuvent présumer que celle-ci ne remplit pas ou ne remplit plus les conditions relatives à la durée du séjour autorisé sur le territoire des États membres. Si cette présomption est renversée, les autorités compétentes créent un dossier individuel pour cette personne dans l'EES, mettent à jour sa dernière fiche d'entrée/de sortie en y ajoutant les données manquantes, ou effacent un fichier existant lorsque l'article 35 du règlement (UE) 2017/2226 le prévoit. (Article 20 du règlement (UE) 2017/2226)
Critères d'inscription dans ce fichier	- Personne ressortissante d'un pays tiers, ou ressortissante d'Islande, du Liechtenstein, de Norvège et de Suisse, admise pour un court séjour au sein de l'espace Schengen (soit pendant un maximum de 90 jours sur une période de 180 jours) et étant soumise à un contrôle à une frontière à laquelle l'EES est mis en œuvre - Personne ressortissante d'un pays tiers, non titulaire d'une carte ou d'un titre de séjour, entrant ou sortant du territoire des États membres et étant membre de la famille d'une personne citoyenne de l'Union à laquelle s'applique la directive 2004/38/CE ou d'une personne ressortissante de pays tiers jouissant d'un droit à la libre circulation équivalent à celui d'une personnes citoyennes de l'Union en vertu d'un accord entre l'Union et ses États membres et un pays tiers - Personne ressortissante d'un pays tiers dont l'entrée sur le territoire des États membres a été refusée (Article 2 du règlement (UE) 2017/2226)

Autorité(s) compétente(s)	EU-Lisa est l'agence chargée de développer le système EES, d'assurer sa gestion opérationnelle (Article 5 du règlement (UE) 2017/2226) et d'héberger le système central de l'EES (Article 7 du règlement (UE) 2017/2226).
Qui a accès à ce fichier ?	- Les autorités nationales compétentes désignées par chaque État membre mettant en œuvre l'EES au sein des autorités frontalières, des autorités chargées des visas et des autorités chargées de l'immigration. La liste des autorités désignées par les États membres doit être communiquée à l'EU-Lisa. L'article 32 du règlement (UE) 2017/2226 fixe les conditions d'accès aux données de l'EES pour les autorités désignées par les États membres. - En vertu de l'article 30 du règlement (UE) 2017/2226, une des unités opérationnelles d'Europol désignée est autorisée à demander l'accès à l'EES à des fins de « prévention » et « détection des infractions terroristes ou d'autres infractions pénales graves, ainsi que les enquêtes en la matière ». L'article 33 du règlement (UE) 2017/2226 fixe les conditions d'accès aux données de l'EES pour Europol. - Certaines données stockées dans l'EES peuvent être transférées à un pays tiers, à des organisations internationales (le HCR, l'OIM et le Comité de la Croix-Rouge) et à des entités privées sous certaines conditions, listées aux articles 41 et 42 du règlement (UE) 2017/2226.
Durée de conservation des données	- Les fiches d'entrée et de sortie ou de refus d'entrée rattachées à un dossier individuel au sein de l'EES sont conservées dans le système central pendant 3 ans suivant la date de la fiche de sortie ou de refus d'entrée. - Les dossiers individuels et les fiches d'entrée et de sortie ou de refus d'entrée rattachées sont conservées dans le système central de l'EES pendant 3 ans et un jour suivant la date de la dernière fiche de sortie ou de refus d'entrée, si aucune fiche d'entrée n'a été enregistrée entre-temps. - Si aucune fiche de sortie n'est enregistrée après la date d'expiration de la durée du séjour autorisé, les données sont conservées durant 5 ans après cette date d'expiration. Les États membres sont prévenus automatiquement par l'EES de la suppression de ces données 3 mois à l'avance. - Pour les personnes ressortissantes de pays tiers qui sont membres de la famille d'une personne citoyenne de l'UE à laquelle s'applique la directive 2004/38/CE ou d'une personne ressortissante de pays tiers jouissant d'un droit à la libre circulation équivalent à celui des citoyens et citoyennes de l'UE et qui ne sont pas titulaires d'une carte ou d'un titre de séjour dans les États membres, chaque fiche d'entrée et de sortie est conservée durant une durée maximale d'1 an après leur sortie du territoire d'un État membre. En l'absence de fiche de sortie, les données sont conservées durant 5 ans à compter de la dernière fiche d'entrée. À la fin de la durée de conservation, les données sont automatiquement effacées du système central de l'EES. (Article 34 du règlement (UE) 2017/2226) L'article 28 du règlement (UE) 2017/2226 dispose que les données extraites de l'EES à des fins d'examen des demandes de visa, des demandes d'accès aux programmes nationaux d'allègement des formalités, de vérification sur le territoire des États membres et d'identification peuvent être conservées « *dans des fichiers nationaux [...] lorsque cela est nécessaire dans un cas particulier, conformément à la finalité pour laquelle elles ont été extraites et conformément aux dispositions pertinentes du droit de l'Union, notamment en matière de protection des données, et pour une durée n'excédant pas ce qui est strictement nécessaire dans le cas concerné* ». L'article 40 du règlement (UE) 2017/2226 précise que la conservation des données introduites par les États membres dans leurs systèmes et fichiers nationaux équivalents doit se faire dans le respect du droit de l'Union et pour une durée n'excédant pas la durée maximale de ces données dans l'EES.
Échanges de données	Le système EES est conçu afin de permettre l'interopérabilité* avec le fichier VIS. Un canal de communication entre les systèmes centraux des deux fichiers doit être établi par l'EU-Lisa afin de permettre la consultation* directe, dans les conditions prévues dans le règlement (UE) 2017/2226 ainsi que le règlement (CE) n°767/2008 et l'extraction, l'importation et la mise à jour des données relatives aux visas depuis le VIS dans l'EES (Article 8 du règlement (UE) 2017/2226). L'EES est connecté au CIR, dans la mesure où lorsque des données sont ajoutées, modifiées ou supprimées dans l'EES, elles le sont également de manière automatique dans le dossier individuel du CIR (Article 19 du règlement (UE) 2019/817).
Comment obtenir communication et rectification des données ?	Les demandes relatives aux droits d'accès, de rectification, à l'effacement et à la limitation doivent être « adressées à l'autorité compétente de tout État membre »[34] (Article 52, paragraphe 1 du règlement (UE) 2017/2226) Par ailleurs, toute personne ayant subi des dommages matériels ou immatériels liés à une opération de traitement non conforme au règlement (UE) 2017/2226, a le droit d'obtenir réparation de l'État membre responsable, et les actions en réparation intentées à l'encontre de cet État membre sont régies par les dispositions du droit national. (Article 45 du règlement (UE) 2017/2226)
Remarques	Le Comité de surveillance coordonnée, créé par le Contrôleur européen de la protection des données en 2018, sera chargé de coordonner la surveillance du traitement des données à caractère personnel pour le système EES. Son objectif est de s'assurer que les systèmes d'information à grande échelle des organes et agences de l'UE sont conformes à l'acte juridique qui les établit.

[34] Au moment de la publication de la boîte à fichiers, l'information concernant « l'autorité compétente de tout État membre » en France n'était pas disponible.

	En France, le groupe Thales a été sélectionné par le ministère de l'intérieur afin de livrer les « kiosques de pré-enregistrement » qui seront déployés aux points de passage aux frontières. Dans le cadre de ses visites de zone d'attente, dans des aéroports, l'Anafé a pu constater l'installation de ces bornes. Au moment de la publication de ce document, elles n'étaient pas fonctionnelles. L'Agence des droits fondamentaux de l'Union européenne est actuellement en train de mener une enquête afin d'examiner les potentiels impacts du système EES sur les droits fondamentaux.
Textes qui régissent ce fichier	- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) - Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 - Règlement (UE) 2024/1356 du Parlement européen et du Conseil du 14 mai 2024 établissant le filtrage des ressortissants de pays tiers aux frontières extérieures et modifiant les règlements (CE) n° 767/2008, (UE) 2017/2226, (UE) 2018/1240 et (UE) 2019/817
Sources	European Union, « What is the EES? », 11 février 2025 Hess Amandine, « Système d'entrée/sortie de l'UE : Quelles conséquences pour les ressortissants de pays tiers ? », *Euronews*, 6 mars 2025 Thales, Thales sélectionné pour préparer la France au nouveau système d'entrée / sortie de l'espace Schengen, 22 mars 2021 VisasNews, L'Union européenne reporte officiellement l'ETIAS et l'EES, 7 mars 2025

Nom du fichier	**ETIAS**
Sens de l'acronyme	European Travel Information and Authorisation System (Système européen d'information et d'autorisation concernant les voyages)
Date de création	Le règlement (UE) 2018/1240 a été publié au Journal officiel de l'Union européenne le 19 septembre 2018. Si l'ETIAS devait à l'origine entrer en vigueur au printemps 2025, des contraintes techniques ont provoqué de nombreux reports et il est à ce jour prévu qu'il soit mis en place à la fin de l'année 2026.
Quelle échelle ?	Européenne
Objectifs officiels	L'ETIAS est une autorisation de voyage que les personnes ressortissantes de pays dits tiers exemptées de visa pour entrer sur le territoire Schengen et à Chypre doivent demander. Cette autorisation peut être accordée pour une période allant jusqu'à 3 ans ou jusqu'à expiration du passeport de la personne voyageant. Elle permet également à ces personnes d'entrer sur le territoire des pays appliquant l'ETIAS autant de fois qu'elles le souhaitent, pour un maximum de 90 jours dans une période de 180 jours. Cette autorisation n'exempte pas les voyageurs et voyageuses de remplir les conditions d'entrée dans les pays dans lesquels elles se rendent. L'objectif est de déterminer si la présence d'une personne ressortissante de pays dits tiers sur le territoire d'un État membre « *est susceptible de présenter un risque en matière de sécurité ou d'immigration illégale ou un risque épidémique élevé* » (Article 1 du règlement (UE) 2018/1240) en amont de son arrivée sur le territoire européen. Par ailleurs, l'ETIAS vise à : - Améliorer « *l'efficacité des vérifications aux frontières* » ; - Contribuer aux objectifs du système SIS au regard des signalements de personnes non-admises ou faisant l'objet d'une interdiction de séjour, de personnes recherchées, disparues ou des signalements de personnes « *aux fins de contrôles discrets ou de contrôles spécifiques* » ; - Contribuer « *à la prévention et à la détection des infractions terroristes ou d'autres infractions pénales graves, et aux enquêtes en la matière* ». (Article 4 du règlement (UE) 2018/1240)
Objectif implicite	Restreindre et contrôler davantage le nombre de personnes étrangères autorisées à entrer sur le territoire Schengen et à Chypre.
Contenu des données	Les données personnelles qui doivent être fournies par la personne demandeuse via le formulaire de demande d'autorisation de voyage en ligne sont : - Une déclaration d'authenticité, d'exhaustivité, d'exactitude et de fiabilité des données fournies ainsi qu'une déclaration de véracité et de fiabilité des déclarations - Des données à caractère personnel : nom(s), prénom(s), date lieu et pays de naissance, sexe, nationalité(s) prénom(s) des parents de la personne demandeuse - Données relatives au document de voyage : type, numéro et pays de délivrance, date de délivrance, date d'expiration - Adresse

	- Adresse électronique et numéro de téléphone - Études - Profession - État membre du premier séjour envisagé (et, à titre facultatif, adresse du premier séjour envisagé) - Pour les personnes mineures : coordonnées de la personne exerçant l'autorité parentale ou tutrice légale - Si la personne demandeuse fait valoir la qualité de membre de la famille d'une personne citoyenne de l'UE : identité et coordonnées du ou de la membre de la famille et liens familiaux - Si la demande est effectuée par une personne autre que la personne demandeuse d'autorisation : identité, coordonnées, lien avec la personne demandeuse et déclaration de représentation signée Les réponses aux questions relatives à : - Une condamnation pénale au cours des 10 années précédentes, ou des 20 années précédentes dans le cas d'une infraction terroriste et date et lieu de l'infraction - Des informations sur le séjour dans une zone de guerre ou de conflit au cours des 10 années précédentes, et raisons de ce séjour - Un ordre de quitter le territoire d'un État membre ou « de tout pays tiers énuméré à l'annexe II du règlement (CE) n°539/2001 » ou décision de retour au cours des 10 années précédentes L'adresse IP à partir de laquelle le formulaire est soumis est relevée par le système d'information* ETIAS. (Article 17 du règlement (UE) 2018/1240) Les données ensuite conservées par le système central ETIAS incluent, en plus des données ci-dessus : - Le numéro de la demande - Des informations sur le statut de la procédure - La date et l'heure de la soumission du formulaire et une mention indiquant le paiement des droits d'autorisation de voyage (7 euros pour les personnes non exemptées en vertu de l'article 18) et le numéro de référence du paiement (Article 19 du règlement (UE) 2018/1240) Des données supplémentaires peuvent être requises auprès de la personne lors du traitement de sa demande, en vertu de l'article 27 du règlement (UE) 2018/1240. Après une prise de décision concernant l'octroi ou non d'une autorisation de voyage, les informations suivantes sont ajoutées au dossier : - Informations sur le statut de la procédure et l'unité délivrant ou refusant l'autorisation (système central ETIAS ou unité nationale ETIAS) - La date de la décision - Le cas échéant, les dates de début et d'expiration de l'autorisation - Le cas échéant, les motifs du refus de l'autorisation - Toute mention dont est assortie l'autorisation de voyage en application de l'article 36, paragraphes 2 et 3, et les motifs de cette mention - Les motifs de la décision finale de l'unité nationale ETIAS de l'État membre responsable du traitement de la demande (Article 39 du règlement (UE) 2018/1240) Une annulation ou une révocation d'une autorisation de voyage et leurs motifs sont également indiqués dans le dossier de la personne voyageuse, avec la date de la décision et le nom et l'adresse de l'unité nationale ETIAS ayant pris cette décision. (Articles 40, 41, 43 du règlement (UE) 2018/1240) Figure également au dossier de la personne voyageuse dans le dossier de la personne voyageuse, le cas échéant, une mention indiquant si l'autorisation de voyage a été délivrée pour des motifs humanitaires, pour des raisons d'intérêt national ou en vertu d'obligations internationales, et les informations relatives à cette décision. (Article 44 du règlement (UE) 2018/1240)
Critères d'inscription dans ce fichier	Personne ressortissante d'un pays dit tiers soumise à l'obligation de détenir une autorisation de voyage et ayant rempli le formulaire de demande d'autorisation de voyage en ligne via le site internet ou l'application* (Article 15 du règlement (UE) 2018/1240).

	Les personnes soumises à l'obligation d'une autorisation de voyage sont : - Les personnes ressortissantes de pays dits tiers qui sont exemptées de l'obligation de visa pour des séjours sur le territoire des États membres d'une durée n'excédant pas 90 jours sur une période de 180 jours (pays listés à l'annexe II du règlement (CE) n° 539/2001) ; - Les personnes qui, en application de l'article 4 paragraphe 2 du règlement (CE) n° 539/2001 sont exemptées de l'obligation de visa pour le même type de séjour ; - Les membres de la famille de personnes citoyennes de l'UE ou d'une personne ressortissante de pays dits tiers jouissant d'un droit à la libre circulation. (Article 2 du règlement (UE) 2018/1240)
Autorité(s) compétente(s)	- L'Agence européenne de garde-frontières et de garde-côtes (Frontex) est responsable du traitement des données à caractère personnel dans le système central ETIAS. - L'EU-Lisa est responsable de la gestion de la sécurité de l'information dans le système central ETIAS. - Les unités nationales ETIAS sont responsables du traitement des données à caractère personnel dans le système central ETIAS par l'État membre auquel elles sont rattachées. (Article 57 du règlement (UE) 2018/1240)
Qui a accès à ce fichier ?	Ont accès à ce fichier : - Le personnel autorisé de l'unité centrale et des unités nationales de l'ETIAS ; - Les autorités frontalières afin d'obtenir le statut de l'autorisation de voyage d'une personne présente à un point de passage des frontières extérieures et aux données de l'article 47, paragraphe 2, points a), c) et d) du règlement (UE) 2018/1240. Les autorités frontalières sont également informées automatiquement des mentions visées à l'article 36, paragraphes 2 et 3 et des motifs de ces mentions. Dans des cas exceptionnels, les autorités frontalières ont également accès aux informations visées à l'article 39, paragraphe 1, point e) ou à l'article 44, paragraphe 6, point f) ; - Les transporteurs afin de consulter le statut de l'autorisation de voyage d'un voyageur ; - Les autorités chargées de l'immigration afin de consulter le statut de l'autorisation de voyage d'un voyageur et certaines données visées à l'article 49 ; - Europol. (Articles 13 et 45 à 53 du règlement (UE) 2018/1240) En cas de correspondance entre des données figurant dans le système ETIAS et des données figurant dans le SIS relatives à des signalements concernant une personne disparue, recherchée ou aux fins de contrôles discrets ou spécifiques, le système central ETIAS envoie une notification automatisée au bureau SIRENE de l'État membre qui a introduit le signalement, incluant certaines données à caractère personnel listées à l'article 23 du règlement (UE) 2018/1240. En vertu de l'article 65 du règlement (UE) 2018/1240, les données à caractère personnel conservées dans le système central ETIAS « ne peuvent être transférées à un pays tiers, une organisation internationale ou une entité privée quelconque, ni être mises à leur disposition, à l'exception des transferts de données à Interpol aux fins de la réalisation du traitement automatisé en application de l'article 20, paragraphe 2, points b) et l), du présent règlement ». Toutefois, à des fins de retours, les autorités chargées de l'immigration peuvent transférer certaines données consultées dans le système central ETIAS à un pays dit tiers. Il faut qu'un ensemble de conditions soient réunies à savoir : - Une recherche préalable a été effectuée dans l'EES et cette recherche indique que l'EES ne contient pas de données concernant le ressortissant de pays tiers devant faire l'objet d'un retour. Et si une des conditions suivantes est remplie : - La Commission a adopté une décision constatant un niveau de protection adéquat des données à caractère personnel dans ce pays tiers, conformément à l'article 45, paragraphe 3, du règlement (UE) 2016/679 ; - Des garanties appropriées ont été fournies, conformément à l'article 46 du règlement (UE) 2016/679, par exemple au moyen d'un accord de réadmission qui est en vigueur entre l'Union ou un État membre et le pays tiers concerné ; - Ou que le transfert des données soit nécessaire pour des raisons importantes d'intérêt public (article 49, paragraphe 1, point d) du RGPD*).
Durée de conservation des données	Les données contenues dans le système central ETIAS sont conservées pendant : - La durée de validité de l'autorisation de voyage ; - 5 ans à compter de la dernière décision de refus, d'annulation ou de révocation de l'autorisation de voyage ; - Si les données figurant dans l'un des systèmes d'information de l'UE ou dans les données d'Europol ou Interpol et étant à l'origine de la décision relative à l'autorisation de voyage sont effacées avant la fin du délai de 5 ans, le dossier de demande est effacé dans un délai de 7 jours à compter de l'effacement de ces données ;

	- Si la personne demandeuse a donné son consentement, les données peuvent être conservées pour un maximum de 3 année supplémentaire après l'expiration de l'autorisation afin de faciliter une nouvelle demande. (Article 54 du règlement (UE) 2018/1240)
Échanges de données	Il existe une interopérabilité* du système ETIAS avec « les autres systèmes d'information de l'Union européenne », soit les systèmes SIS II, VIS, EES, EURODAC et ECRIS-TCN et les données d'EUROPOL (Article 11 du règlement (UE) 2018/1240). Le système central ETIAS interroge également les fichiers d'INTERPOL sur les documents de voyage volés (SLTD) et sur les documents de voyages associés aux notices (TDAWN). Les modalités des échanges de données et des informations consultées par le système central ETIAS dans ces autres traitements sont listées aux articles 20, 22, 23 et 29 du règlement (UE) 2018/1240. L'ETIAS est connecté au CIR, dans la mesure où lorsque des données sont ajoutées, modifiées ou supprimées dans l'ETIAS, elles le sont également de manière automatique dans le dossier individuel du CIR. (Article 19 du règlement (UE) 2019/817)
Comment obtenir communication et rectification des données ?	Pour exercer les droits d'accès, de rectification, d'effacement et à la limitation du traitement des données, les personnes demandeuses peuvent s'adresser à l'unité centrale ETIAS ou l'unité nationale ETIAS de l'État membre responsable de leur demande. (Article 64 du règlement (UE) 2018/1240) Sur le site de l'UE voyage : « *Si votre demande d'autorisation ETIAS est refusée ou si votre autorisation de voyage ETIAS est annulée ou révoquée, vous recevrez un e-mail indiquant les motifs de la décision et l'autorité qui a pris la décision. Vous avez le droit de faire appel : le courrier électronique contiendra des informations sur les pays européens auxquels vous devez faire appel et décrire la procédure pertinente. Les recours sont traités conformément à la législation nationale de ces pays. Si votre autorisation de voyage est révoquée à votre demande, il n'est pas possible de faire appel de la décision.* »
Remarques	Les personnes doivent remplir un formulaire en ligne sur l'application* ETIAS. Les frais de dossier sont de 7 euros. Il semblerait que dans certains cas, il soit possible d'obtenir un rendez-vous en ambassade ; cependant des guichets ou une possibilité physique ne semblent pas être prévus dans le cadre du déploiement d'ETIAS (UE, *ETIAS : Ce dont vous avez besoin pour postuler*, 2025) En vertu de l'article 7 du règlement (UE) 2018/1240, une unité centrale ETIAS est créée au sein de Frontex. En vertu de l'article 10 du règlement (UE) 2018/1240, un comité d'orientation ETIAS sur les droits fondamentaux indépendant doit être institué et avoir un rôle de conseil et d'évaluation. Ce comité est composé de l'officier aux droits fondamentaux de Frontex, d'un représentant du Forum consultatif sur les droits fondamentaux de Frontex, d'un représentant du Contrôleur européen de la protection des données, d'un représentant du comité européen de la protection des données et d'un représentant de l'Agence des droits fondamentaux de l'Union européenne. Ce comité doit se réunir au moins deux fois par an et « chaque fois que cela est nécessaire » afin d'évaluer l'impact du traitement des données dans le système ETIAS sur les droits fondamentaux, et notamment le respect de la vie privée, la protection des données à caractère personnel et la non-discrimination. Le comité est chargé de publier un rapport annuel, mis à disposition du public. En vertu des articles 34 et 35 du règlement (UE) 2018/1240, une « liste de surveillance ETIAS » est créée au sein du système central ETIAS, regroupant des « *données relatives à des personnes soupçonnées d'avoir commis une infraction terroriste ou une autre infraction pénale grave ou d'y avoir participé, ou à des personnes pour lesquelles il existe des indices concrets ou des motifs raisonnables permettant de croire, sur la base d'une évaluation globale de la personne, qu'elles commettront une infraction terroriste ou une autre infraction pénale grave* ». Les informations relatives à ces infractions terroristes ou pénales sont introduites dans la liste par Europol ou les États membres. L'article 56 de la loi n° 2024-42 du 26 janvier 2024 introduit en France le système ETIAS.
Textes qui régissent ce fichier	- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil - Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données - Règlement (CE) n° 539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des États membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

	- 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 - Règlement (UE) 2018/1240 du Parlement Européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n°1077/2011, (UE) n°515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 - Règlement (UE) 2024/1356 du Parlement européen et du Conseil du 14 mai 2024 établissant le filtrage des ressortissants de pays tiers aux frontières extérieures et modifiant les règlements (CE) n° 767/2008, (UE) 2017/2226, (UE) 2018/1240 et (UE) 2019/817
Sources	Légifrance, voir ci-dessus les « Textes qui régissent ce fichier » European Union, « What is ETIAS », février 2025 VisasNews, « L'Union européenne reporte officiellement l'ETIAS et l'EES », mars 2025 UE, *ETIAS : Ce dont vous avez besoin pour postuler*, 2025

Nom du fichier	**EURODAC**
Sens de l'acronyme	EU biometric DataBase (Système de comparaison des empreintes digitales des demandeurs d'asile) Eurodac est composé : - D'un système central comprenant : une unité centrale, un plan et un système de maintien des activités ; - D'une infrastructure de communication entre le système central et les États membres, qui fournit un canal de communication sécurisé et crypté pour les données d'Eurodac ; - Du CIR (répertoire commun de données d'identité) ; - D'une infrastructure de communication sécurisée entre le système central et les infrastructures centrales du portail de recherche européen et entre le système central et le CIR.
Date de création	11 décembre 2000
Quelle échelle ?	Européenne
Objectifs officiels	Eurodac est un système d'information à grande échelle contenant les empreintes digitales des personnes en demande d'asile et de protection subsidiaire et les personnes en situation dite irrégulière se trouvant sur le territoire de l'UE. Le fichier organise la conservation des empreintes digitales pour appliquer la procédure « Dublin » dans l'Union européenne (qui concerne les personnes ressortissantes de pays dits tiers qui veulent déposer une demande d'asile). (Article 20 du règlement n° 603/2013) Selon l'article 1 du règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'« Eurodac » pour la comparaison des données biométriques* aux fins de l'application efficace du règlement (UE) 2024/1351, Eurodac a pour objectif de : - Soutenir le système d'asile, y compris en contribuant à déterminer l'État membre qui est responsable de l'examen d'une demande de protection internationale enregistrée dans un État membre par une personne ressortissante de pays dit tiers ou apatride ; - Contribuer au contrôle de l'immigration irrégulière vers l'Union, à la détection des mouvements secondaires au sein de celle-ci et à l'identification des personnes ressortissantes de pays dits tiers et apatrides en séjour dit irrégulier, afin de définir les mesures qui doivent être prises par les États membres ; - Contribuer à la protection des enfants, y compris à des fins répressives ; - Définir les conditions dans lesquelles les autorités désignées des États membres et l'autorité désignée d'Europol peuvent demander la comparaison de données biométriques* ou alphanumériques* avec celles conservées dans Eurodac à des fins répressives, en vue de la prévention et de la détection d'infractions terroristes ou d'autres infractions pénales graves, ou en vue des enquêtes en la matière ; - Contribuer à l'identification correcte des personnes enregistrées dans Eurodac conformément à l'article 20 du règlement (UE) 2019/818 en conservant des données d'identité, des données du document de voyage et des données biométriques* dans le répertoire commun de données d'identité (CIR) ; - Appuyer les objectifs du système européen d'information et d'autorisation concernant les voyages (ETIAS) ; - Appuyer les objectifs du système d'information* sur les visas (VIS) ; - Soutenir l'élaboration de politiques fondées sur des données factuelles par la production de statistiques ; - Contribuer à la mise en œuvre de la Directive 2001/55/CE.

	Ainsi, de manière générale le fichier Eurodac permet selon la communication de l'UE : « *de vérifier si un demandeur ou une personne en séjour irrégulier dans un État membre a déjà demandé l'asile dans un autre État membre, de vérifier si un demandeur a déjà été appréhendé lors de son entrée irrégulière sur le territoire européen, d'appliquer les critères pertinents pour déterminer quel État membre est responsable de l'examen d'une demande d'asile* ». Il est d'ailleurs précisé que : « *En élargissant la base de données Eurodac afin de collecter davantage de données et d'inclure davantage de catégories de migrants, l'UE peut mieux suivre les mouvements irréguliers et surveiller les parcours des demandeurs d'asile.* »
Objectifs implicites	Comme le rappellent 110 organisations de la société civile, dont Statewatch et European Digital Rights : « *Dès le début, ce système a été un moyen d'appliquer un régime d'expulsion discriminatoire et nuisible, fondé sur un faux cadre d'« illégalité » dans la migration. Après une première réforme en 2013 permettant à la police d'accéder à la base de données, l'UE continue de détacher Eurodac de son cadre d'asile pour le reconditionner en un système poursuivant des « objectifs d'immigration plus larges ». Les changements ont été annoncés en 2020 dans le pacte migratoire de l'UE, le soi-disant « nouveau départ en matière de migration » de l'UE. Plutôt qu'un nouveau départ, les propositions contiennent les propositions les plus dures de l'histoire de la politique migratoire de l'UE : plus de détention, plus de violence et un outil de surveillance plus large et évolué dans la base de données Eurodac pour suivre, refouler et expulser les migrants « en situation irrégulière ».* » Ces organisations soulignent que « *la réforme d'Eurodac est une violation flagrante du droit de demander une protection internationale, un amalgame effrayant entre migration et criminalité et un instrument de surveillance incontrôlable. L'extrême droite anticipe déjà la prochaine étape, en appelant à la collecte d'ADN. La réforme d'EURODAC est l'un des nombreux exemples de la numérisation de la forteresse Europe. Elle est incompatible avec les droits fondamentaux et portera atteinte aux cadres de protection et aux droits des personnes en mouvement.* » (Statewatch, Europe's (digital) borders must fall: End the expansion of the EU's EURODAC database, 2023) Enfin Statewatch dénonce : « *le règlement Eurodac remanié, le règlement sur le filtrage, le code frontières Schengen révisé et la loi sur l'intelligence artificielle. La proposition de transformer [et actuelle transformation] Eurodac permettrait de collecter davantage de types de données auprès d'un groupe beaucoup plus large de personnes (tous les migrants en situation irrégulière, ainsi que les demandeurs d'asile), en vue de les stocker dans une base de données élargie qui, à son tour, fera partie de l'architecture d'interopérabilité* de l'UE, facilitant ainsi la recherche et l'interconnexion de différents ensembles de données. Le règlement sur le filtrage introduira des contrôles obligatoires dans les bases de données européennes et internationales pour toutes les personnes qui franchissent illégalement les frontières extérieures, et dont il est de plus en plus probable qu'elles se retrouvent en détention.* » (Statewatch, *Le numérique et les frontières européennes*, Rapport, 2024) Le réseau Migreurop analysait en 2020 que « *Les données récoltées alimentent des bases de données sur les demandes d'asile comme Eurodac, dont l'utilisation n'est pas circonscrite à ce domaine, par exemple si ces données permettent de confirmer l'identité d'une personne avant son expulsion* ». (Migreurop, Data et nouvelles technologies : la face cachée du contrôle des mobilités, 2020)
Contenu des données	Les données sont relevées pour toute personne d'au moins 6 ans et sont envoyées à l'unité centrale par des points d'accès nationaux. Le fichier Eurodac bénéficie d'un système informatisé de reconnaissance digitale et faciale. (Voir notamment l'article 37 du règlement (UE) 2024/1358) **Pour les personnes demandant une protection internationale :** - Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe - L'État membre d'origine, le lieu et la date de l'enregistrement ; - Lorsqu'un tel document est disponible, le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, lorsqu'un tel document est disponible, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document facilitant l'identification du ressortissant de pays tiers ou de l'apatride, accompagné d'indications portant sur son authenticité ; - Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur ; - La date à laquelle une protection internationale ou un statut humanitaire au titre du droit national a été accordé. (Article 21 du règlement (UE) 2024/1358) **Pour les personnes enregistrées aux fins de l'exécution d'une procédure d'admission et personnes admises conformément à un programme de réinstallation national :**

	- Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe - L'État membre d'origine, le lieu et la date de l'enregistrement conformément à l'article 9, paragraphe 3, du règlement (UE) 2024/1350 ; - Lorsqu'un tel document est disponible, le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, lorsqu'un tel document est disponible, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document facilitant l'identification du ressortissant de pays tiers ou de l'apatride, accompagné d'indications portant sur son authenticité ; - Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur ; - Le cas échéant, la date de la décision d'accorder une protection internationale ou un statut humanitaire au titre du droit national conformément à l'article 9, paragraphe 14, du règlement (UE) 2024/1350 ; - Le cas échéant, la date de refus d'admission conformément au règlement (UE) 2024/1350 et les motifs pour lesquels l'admission a été refusée ; - Le cas échéant, la date de l'interruption de la procédure d'admission visée dans le règlement (UE) 2024/1350. (Article 19 du règlement (UE) 2024/1358) **Pour les personnes ressortissantes de pays dits tiers ou apatrides interpellées lors du franchissement en dehors des postes frontières habilités à une frontière extérieure :** - Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe ; - L'État membre d'origine, le lieu et la date d'interpellation ; - Lorsqu'un tel document est disponible, le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, lorsqu'un tel document est disponible, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document facilitant l'identification du ressortissant de pays tiers ou de l'apatride, accompagné d'indications portant sur son authenticité ; - Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur. - La date à laquelle la personne concernée a quitté le territoire des États membres ou en a été éloignée ; - L'État membre de relocalisation ; - Le fait que l'AVVR (assistance au retour volontaire et à la réintégration) a été accordée ; - Le fait que la personne est susceptible de constituer une menace pour la sécurité intérieure, à la suite du filtrage visé dans le règlement (UE) 2024/1356, si l'une des circonstances suivantes s'applique : la personne concernée est armée, la personne concernée est violente, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées dans la directive (UE) 2017/541, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI. (Article 22 du règlement (UE) 2024/1358) **Pour les personnes ressortissantes de pays dits tiers ou apatrides en séjour irrégulier sur le territoire d'un État membre :** - Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe ; - L'État membre d'origine, le lieu et la date d'interpellation ; - Lorsqu'un tel document est disponible, le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, lorsqu'un tel document est disponible, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document facilitant l'identification du ressortissant de pays tiers ou de l'apatride, accompagné d'indications portant sur son authenticité ;

	- Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur ; - La date à laquelle la personne concernée a quitté le territoire des États membres ou en a été éloignée ; - L'État membre de relocalisation ; - La date d'arrivée de la personne concernée à la suite d'un transfert réussi ; - Le fait que l'AVVR (assistance au retour volontaire et à la réintégration) a été accordée ; - Le fait que la personne est susceptible de constituer une menace pour la sécurité intérieure, à la suite du filtrage visé dans le règlement (UE) 2024/1356, si l'une des circonstances suivantes s'applique : la personne concernée est armée, la personne concernée est violente, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées dans la directive (UE) 2017/541, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI. (Article 23 du règlement (UE) 2024/1358) **Pour le débarquement de personnes étrangères à la suite d'une opération de sauvetage :** - Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe ; - L'État membre d'origine, le lieu où l'intéressé a été débarqué et la date ; - Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur ; - Le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document facilitant l'identification du ressortissant de pays tiers ou de l'apatride, accompagné d'indications portant sur son authenticité ; - La date à laquelle la personne concernée a quitté le territoire des États membres ou en a été éloignée ; - L'État membre de relocalisation - Le fait que l'AVVR (assistance au retour volontaire et à la réintégration) a été accordée ; - Le fait que la personne est susceptible de constituer une menace pour la sécurité intérieure, à la suite du filtrage visé dans le règlement (UE) 2024/1356, si l'une des circonstances suivantes s'applique : la personne concernée est armée, la personne concernée est violente, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées dans la directive (UE) 2017/541, il existe des éléments indiquant que la personne concernée est impliquée dans l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI. (Article 24 du règlement (UE) 2024/1358) **Pour les bénéficiaires d'une protection internationale :** - Les données dactyloscopiques ; une image faciale ; les nom(s) et prénom(s), nom(s) à la naissance, noms utilisés antérieurement et pseudonymes, qui peuvent être saisis séparément ; la ou les nationalités ; la date et le lieu de naissance ; le sexe ; - L'État membre d'origine, le lieu et la date d'enregistrement de la personne concernée en tant que bénéficiaire d'une protection temporaire ; - Lorsqu'un tel document est disponible, le type et le numéro du document d'identité ou de voyage ; le code en trois lettres du pays de délivrance et la date d'expiration dudit document ; - Une copie couleur scannée d'un document d'identité ou de voyage, lorsqu'un tel document est disponible, accompagnée d'indications portant sur son authenticité, ou, à défaut, un autre document ; - Le numéro de référence attribué par l'État membre d'origine ; la date à laquelle les données biométriques ont été relevées ; la date à laquelle les données ont été transmises à Eurodac ; le code d'identification de l'opérateur ; - Le cas échéant, le fait que la personne précédemment enregistrée en tant que bénéficiaire d'une protection temporaire relève de l'un des motifs d'exclusion prévus à l'article 28 de la directive 2001/55/CE ; - La référence de la décision d'exécution du Conseil pertinente. (Article 26 du règlement (UE) 2024/1358)

Critères d'inscription dans ce fichier	Personne d'au moins 6 ans ayant : - Déposé une demande d'asile dans un des États membre de l'Espace Schengen ; - Été appréhendée lors du franchissement en dehors des postes frontières habilités d'une frontière extérieure de l'UE ; - Été appréhendée en situation d'irrégularité sur le territoire d'un État membre ; - Lors du débarquement à la suite d'une opération de recherche et sauvetage ; - Enregistrée aux fins de l'exécution d'une procédure d'admission et une personne admise conformément à un programme de réinstallation nationale. Les empreintes sont collectées, de manière obligatoire (Article 13 du règlement (UE) 2024/1358 sur l'obligation de relever les données biométriques) sur des personnes âgées d'au moins 6 ans.
Autorité(s) compétente(s)	**Au niveau européen** : le système est composé d'une unité centrale équipée d'un système informatisé de reconnaissance des empreintes digitales. L'agence EU-Lisa gère l'aspect opérationnel de la base de données centrale pour le compte des États membres et effectue des statistiques. **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 également procéder à une inscription.
Qui a accès à ce fichier ?	Chaque État membre désigne et notifie à l'agence EU-Lisa 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 : 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) ; - 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) ; - Selon le règlement (UE) 2024/1358, les autorités compétentes chargées des visas peuvent consulter Eurodac.
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 10 ans à compter de la date de transmission des données biométriques. - Les données enregistrées dans le cadre d'une procédure d'admission au titre du cadre de l'Union pour la réinstallation et l'admission humanitaire et à laquelle cet État membre accorde une protection internationale ou un statut humanitaire au titre du droit national sont conservées 5 ans à compter de la date de transmission des données biométriques. Si l'État membre n'a pas accordé une protection internationale ou a interrompu la procédure les données sont conservées 3 ans à compter de la date de transmission des données biométriques. - Lorsqu'une personne ressortissante de pays dit tiers ou apatride s'est vu opposer un refus d'admission par un État membre, les données sont conservées 3 ans à compter de la date à laquelle l'admission a fait l'objet d'une conclusion négative. - Pour les personnes enregistrées dans EURODAC en situation d'irrégularité sur le territoire d'un État membre, les données sont conservées 5 ans. Passé ces délais, les données sont automatiquement effacées du système central. Les données concernant une personne demandeuse 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 État membre de l'Union européenne font également l'objet d'un effacement automatique anticipé.
Échanges de données ?	- Interopérabilité* avec ETIAS: « *À partir du 12 juin 2026, Eurodac est connecté au portail de recherche européen visé à l'article 6 du règlement (UE) 2019/818 afin de permettre l'application des articles 11 et 20 du règlement (UE) 2018/1240.* » (Article 8 du règlement (UE) 2024/1358) - Interopérabilité* avec le VIS (Article 11 du règlement (UE) 2024/1358) - On peut également noter, à l'aide de la communication de l'UE sur la mise à jour de la base de données européennes des empreintes digitales, une interconnexion avec le SIS II (Système d'information Schengen). - Au travers du CIR, EURODAC a accès aux données de l'ECRIS-TCN et l'EES.
Comment obtenir communication et rectification des données ?	L'État membre à l'origine de l'enregistrement dans EURODAC doit informer la personne concernée du présent règlement, par écrit, et, si nécessaire, oralement, dans une langue qu'elle comprend ou dont on peut raisonnablement supposer qu'elle la comprend, sous une forme concise, transparente, intelligible et aisément accessible, dans un langage clair et simple. (Article 42 concernant le Droit à l'information du règlement (UE) 2024/1358)

	Toute personne peut accéder aux données la concernant, ainsi qu'à l'identité de l'État membre ayant transmis ces données au système central. L'État membre d'origine est seul habilité à modifier, en les rectifiant ou en les complétant, les données qu'il a transmises à Eurodac, ou à les effacer, sans préjudice de l'effacement effectué en vertu de l'article 29. Lorsque les droits de rectification et d'effacement des données à caractère personnel sont exercés dans un État membre autre que celui ou ceux qui ont transmis les données, **les autorités dudit État membre prennent contact avec les autorités de l'État membre ou des États membres qui ont transmis les données afin qu'elles puissent vérifier l'exactitude des données et la licéité de leur transmission à Eurodac et de leur enregistrement dans Eurodac.** L'État membre dit d'origine doit confirmer par écrit à la personne concernée qu'il a rectifié, complété ou effacé des données à caractère personnel la concernant ou en a limité le traitement. En France, 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.
Remarques	Il existe des dispositions particulières concernant la collecte des données biométriques* concernant les personnes mineures : « Les données biométriques* des mineurs âgés d'au moins six ans sont recueillies par des fonctionnaires formés spécifiquement pour recueillir les données biométriques* d'un mineur, d'une manière adaptée aux enfants et tenant compte de leur spécificité, dans le plein respect de l'intérêt supérieur de l'enfant et des garanties prévues par la convention des Nations unies relative aux droits de l'enfant. » (Règlement (UE) 2024/1358) De plus, on peut lire dans le guide pour les autorités lors de la prise d'empreintes digitales pour Eurodac (2021) : « Les demandeurs d'asile et les migrants souffrant de handicaps physiques peuvent ne pas être en mesure de fournir leurs empreintes digitales. D'autres pourraient refuser de les donner. En cas de non-respect de l'obligation de fournir des empreintes digitales, la fourniture répétée d'informations et de conseils peuvent réduire le risque de recourir à des mesures coercitives. » L'obligation de collecte des données biométriques, comme l'ensemble des fichiers pour lesquels le droit d'opposition* ne s'applique pas, engendre de fait la coercition par les autorités et questionne sur les pratiques de collectes des données biométriques* par les autorités. En France, le Conseil constitutionnel a censuré une disposition de la loi immigration 2024 sur la prise d'empreintes coercitive sans le consentement de la personne étrangère (Conseil constitutionnel, 25 janvier 2024, n° 2023-863 DC). Si cette censure n'est pas spécifique à Eurodac, cela signifie qu'il risque d'y avoir une difficulté d'application de la nouvelle mouture d'Eurodac. Comme le dénonce, déjà en 2021 avant l'élargissement du nombre de données collectées et du nombre de personnes concernées par ce fichage, « On a vu des migrants refuser de donner leurs empreintes à leur arrivée en Grèce, ou même se brûler les doigts pour ne pas être enregistrés dans Eurodac, rappelle Damien Simonneau, chercheur à l'Institut Convergences Migrations. Ils savent que s'ils ont, par exemple, de la famille en Allemagne, mais qu'ils ont été enregistrés en Grèce, ils seront renvoyés en Grèce pour que leur demande y soit traitée, ce qui a des conséquences énormes sur leur vie. » La procédure d'instruction dure en effet de 12 à 18 mois en moyenne. (InfoMigrants, « Pour les migrants, la biométrie tout au long du chemin », 2021) Comme le rappelle le Gisti dans son article Frénésie sécuritaire : l'algorithme du rejet (2024) : « Le déploiement des fichiers forme in fine un dispositif panoptique dont le fonctionnement opaque rend illusoire l'exercice des garanties théoriquement prévues par les textes au profit des personnes faisant l'objet d'un fichage. En effet, la collecte et l'usage des données personnelles s'effectuent souvent en l'absence de consentement des personnes concernées. On peut ainsi douter que les personnes inscrites au fichier Eurodac soient informées du fait que le logiciel* de reconnaissance faciale, qui sera intégré à cette base de données, est actuellement entraîné à partir de leurs informations personnelles. » Le Comité de surveillance coordonnée, créé par le Contrôleur européen de la protection des données en 2018, sera chargé de coordonner la surveillance du traitement des données à caractère personnel pour la base de données Eurodac. Son objectif est de s'assurer que les systèmes d'information à grande échelle des organes et agences de l'UE sont conformes à l'acte juridique qui les établit.
Textes 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 pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte)

	- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) - Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'« Eurodac » pour la comparaison des données biométriques* aux fins de l'application efficace des règlements (UE) 2024/1351 et (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et 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, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil
Sources	European Union Agency for Fundamental Rights, Le droit à l'information — Guide pour les autorités lors de la prise d'empreintes digitales pour Eurodac, 2021 Gisti, Frénésie sécuritaire : l'algorithme du rejet, 2024 InfoMigrants, « Pour les migrants, la biométrie tout au long du chemin », 2021 Migreurop, Data et nouvelles technologies, la face cachée du contrôle des mobilités, 2020 Statewatch, Schengen and EU extend Fortress Europe (feature), 1998 Statewatch, Europe's (digital) borders must fall: End the expansion of the EU's EURODAC database, 2023 Statewatch, Automating the fortress: digital technologies and European borders, 2024

Nom du fichier	**SIS II**
Sens de l'acronyme	Schengen Information System II (Système d'Information Schengen II)
Date de création	20 décembre 2006
Quelle échelle ?	Européenne
Objectifs officiels	Structure du SIS II : - Le système central = le **SIS central**, contient la base de données SIS II - Le système national dans chaque État membre = le **N-SIS** - 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. Ce fichier a pour objectif de : - Permettre aux États 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 et ressortissantes tout en préservant l'ordre et la sécurité publique ; - 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**. (Paragraphes 1 et 6 du préambule du règlement (UE) 2018/1862)
Objectif implicite/ Remarques	Le fichier SIS II, à l'instar du VIS et d'EURODAC, a pour objectif de lutter entre autres 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 irrégulière ». Il y a un glissement du passage du fichier SIS comme fichier d'identification à un fichier d'enquête policière. (Ségolène Barbou Des Places, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », *in Fichiers informatiques et sécurité publique*, Presses Universitaires de Nancy, 2013).
Contenu des données	Données concernant les personnes signalées dans le SIS central : - 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 genre

	- Les photographies et images faciales - Les empreintes digitales - La ou les nationalités - L'indication que la personne concernée est armée, violente, en fuite, présente un risque de suicide ou une menace pour la santé publique ou est impliquée dans une activité terroriste - Le motif du signalement - L'autorité signalante - Une référence à la décision qui est à l'origine du signalement - La conduite à tenir - Le(s) lien(s) vers d'autres signalements introduits dans le SIS II - Le type d'infraction - Le numéro d'immatriculation de la personne dans un registre national - Pour les signalements visés à l'article 32, paragraphe 1, une catégorisation du type de dossier - La catégorie des documents d'identification de la personne, leur(s) numéro(s) et le pays et la date de délivrance - Les profils ADN pertinents - Les données dactyloscopiques - Une copie des documents d'identification, si possible en couleurs (Article 20 du règlement (UE) 2018/1862) Données dans le N-SIS en France : - L'état civil (noms, prénoms et alias, date et lieu de naissance), le sexe et la nationalité - Les signes physiques particuliers, objectifs et permanents - L'indication que la personne est armée, violente, s'est enfuie ou échappée, présente un risque de suicide, est impliquée dans un acte de terrorisme, est susceptible de constituer une menace pour la santé publique - Le photographies permettant de recourir à un dispositif de reconnaissance faciale et autres photographies - Les empreintes digitales et palmaires - Les empreintes génétiques dans les cas prévus au paragraphe 3 de l'article 42 du règlement (UE) 2018/1862 du 28 novembre 2018 - Le numéro national d'immatriculation de la personne dans un registre étranger pour les signalements - Le motif et la décision à l'origine du signalement - La conduite à tenir vis-à-vis de la personne - Le descriptif et les caractéristiques des objets présentant un lien direct avec cette personne et permettant de la localiser ou un lien avec certaines des infractions commises - Les liens avec d'autres signalements créés dans le SIS - Le type d'infraction - Des informations sur la décision de retour le cas échéant - Des informations sur la décision de non-admission et d'interdiction de séjour le cas échéant - Le numéro du titre d'identité et de voyage et/ou du permis de conduire, leur date et pays de délivrance, une copie de ces titres et le numéro national d'identification étranger (Article R. 231-9 du code de la sécurité intérieure)
Critères d'inscription dans ce fichier	Les États-membres peuvent inscrire une personne dans le SIS si elle appartient à une des catégories suivantes : - Personne disparue ; - Enfant risquant d'être enlevé par un ou une membre de sa famille ou personne tutrice ; - Personne vulnérable risquant de subir la traite des êtres humains ou des violences fondées sur le genre hors du territoire d'un État membre ; - Personne recherchée en vue d'une arrestation ;

	- Personne dont le concours est requis pour une procédure judiciaire ; - Personnes devant faire l'objet d'un contrôle discret, d'investigation ou spécifique ; - Personne recherchée inconnue ; - Personne faisant l'objet d'une décision de retour ; - Personne ressortissante d'un pays dit tiers n'ayant pas le droit d'entrer dans l'espace Schengen et signalée aux fins de non-admission et d'interdiction de séjour. (Règlement (UE) 2018/1862 à partir du chapitre VI) En France, sont inscrites dans le SIS les personnes appartenant à l'une des catégories suivantes : - Les personnes recherchées pour arrestation aux fins d'extradition ; - Les étrangers et étrangères signalées aux fins de non-admission à la suite d'une décision administrative ou judiciaire ; - Les personnes disparues et les personnes qui, dans l'intérêt de leur propre protection ou pour la prévention de menaces, doivent être placées provisoirement en sécurité ; - Les personnes recherchées par l'autorité judiciaire dans le cadre d'une procédure pénale ; - Les personnes recherchées par l'autorité judiciaire pour la notification ou l'exécution d'une décision pénale. (Article R. 231-6 du code de la sécurité intérieure)
Autorité(s) compétente(s)	En France : la direction générale de la police nationale (ministère de l'intérieur) L'EU-Lisa est chargée de la gestion opérationnelle du SIS central et d'assurer la sécurité du SIS central et de l'infrastructure de communication, notamment en ce qui concerne la protection des données. (Articles 15 et 16 du règlement (UE) 2018/1861)
Qui a accès à ce fichier ?	Au niveau français : - Le personnel du bureau SIRENE français (Supplément d'Information Requis à l'Entrée dans un État membre : bureau qui gère la partie nationale N-SIS et destinataire de demandes de signalements effectués en France) et de l'office N-SIS ; - Les personnels de la police nationale, de la gendarmerie nationale, des services des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires ; - Le personnel des services centraux du ministère de l'intérieur et des préfectures et sous-préfectures chargé : - De l'application de la réglementation relative aux personnes étrangères, à l'acquisition de la nationalité française, aux titres d'identité et de voyage, aux permis de conduire, aux visas, ainsi qu'aux armes, munitions et explosifs ; - De l'immatriculation des véhicules ; - Le personnel du ministère de l'Europe et des affaires étrangères chargés du traitement des titres d'identité et de voyage et de l'instruction des demandes de visa ; - Le personnel du service national des enquêtes administratives de sécurité ; - Le personnel de l'agence nationale des données de voyage ; - Le personnel du service national des enquêtes d'autorisation de voyage ; - Le personnel du service central des armes et explosifs ; - Le personnel du commandement spécialisé pour la sécurité nucléaire ; - Le personnel opérationnel du contingent permanent du corps européen de garde-frontières et de garde-côtes. Les autorités judiciaires et les autorités et services homologués des États membres peuvent également être destinataire des données enregistrées dans le N-SIS français. (Article R. 231-10 du code de la sécurité intérieure) Dans les autres États membres de l'UE, ont accès à ce fichier : - Les autorités nationales compétentes légalement désignées à cette fin, notamment les autorités chargées de l'identification de personnes ressortissantes de pays dits tiers, les autorités nationales compétentes en matière de naturalisation, les autorités judiciaires nationales, les autorités nationales chargées des demandes de visa et des décisions d'annulation d'abrogation ou de prolongation, conformément au droit national ; - Europol ; - Les membres nationaux d'Eurojust[35] et leurs personnels assistants ;

[35] Eurojust est l'agence européenne chargée de renforcer la coopération judiciaire entre les États membres, pour les poursuites relatives à la criminalité organisée.

	- Des membres de l'Agence européenne de garde-frontières et de garde-côtes (Frontex), du Bureau européen d'appui en matière d'asile et d'autres agences de l'Union compétentes déployant des experts apportant un renfort technique et opérationnel « *aux États membres dans les zones d'urgence migratoire* ». (Article 17 du règlement (UE) 2018/1860, Article 36 du règlement (UE) 2018/1861, Article 2, points 8) et 9) du règlement (UE) 2016/1624)
Durée de conservation des données	Les signalements sont conservés « *pendant le temps nécessaire à la réalisation des finalités pour lesquelles ils ont été introduits* ». Toutefois, l'État membre ayant introduit le signalement doit le réexaminer dans un délai de 3 ans à compter de son introduction dans le SIS et évaluer la nécessité de le conserver. Le signalement est supprimé si une prolongation n'est pas décidée. (Article 39 du règlement (UE) 2018/1861) Le délai de réexamen est de 5 ans pour les signalements concernant des personnes disparues devant être placées sous protection et les personnes sous mandat d'arrêt. (Article 53 du règlement (UE) 2018/1862) Les données du SIS conservées par les États membres dans leurs fichiers nationaux sur la base desquelles la conduite a été exécutée sur leur territoire peuvent être conservées pour une durée maximale de 3 ans, sauf si des dispositions particulières du droit national prévoient une durée de conservation plus longue. Les États membres ont également le droit de conserver dans leurs fichiers nationaux les données contenues dans les signalements qu'ils ont introduit eux-mêmes dans le SIS. (Article 42 du règlement (UE) 2018/1861) En France, les données relatives aux signalements concernant les personnes peuvent être conservées pour des durées maximales allant de 1 à 5 ans, selon le type de signalement effectué. Les données relatives aux signalements concernant les objets peuvent être conservées pour une durée maximale de 10 ans. Ces durées peuvent être prolongées si jugées nécessaire. (Article R. 231-11 du code de la sécurité intérieure)
Échanges de données ?	Selon la Cnil : Les signalements effectués par l'État 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). Le SIS peut être interrogé via le portail de recherche européen (ESP) (Paragraphe 17 du préambule du règlement (UE) 2019/817). L'ESP comprend une infrastructure de communication sécurisée avec EES, le VIS, ETIAS, EURODAC, le SIS central, ECRIS-TCN, les données Europol et les bases de données d'Interpol, ainsi qu'avec les infrastructures centrales du CIR et du détecteur d'identités multiples (MID), également créé par le règlement (UE) 2019/817 (Article 6 du règlement (UE) 2019/817). Les autorités des États membres et agences de l'Union ayant accès à au moins l'un des systèmes d'information de l'UE peuvent utiliser l'ESP (Article 7 du règlement (UE) 2019/817). Ces autorités peuvent lancer une requête en soumettant les données alphanumériques* ou biométriques* à l'ESP. « *Lorsqu'une requête a été lancée, l'ESP interroge l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN et le CIR ainsi que les données d'Europol et les bases de données d'Interpol, simultanément, à l'aide des données envoyées par l'utilisateur et conformément au profil d'utilisateur.* » Aucune information concernant des données à laquelle l'autorité lançant la requête n'a pas accès en vertu du droit de l'Union ne peut être communiquée par l'ESP (Article 9 du règlement (UE) 2019/817). Le service partagé d'établissement de correspondances biométriques* (BMS), également créé par le règlement (UE) 2019/817, doit être utilisé avec l'ESP afin de comparer les données enregistrées dans le CIR et dans le SIS de manière automatique. Dans l'autre sens, le CIR et le SIS devraient être en mesure d'utiliser le BMS afin de détecter les liens possibles sur la base des données biométriques, et l'ESP pour les liens possibles sur la base des données alphanumériques*. Le CIR et le SIS devraient également pouvoir détecter les données identiques ou similaires relatives à une personne stockées dans plusieurs systèmes (Paragraphe 41 du préambule du règlement (UE) 2019/817). La vérification des différentes identités doit se faire manuellement par l'autorité nationale ou l'agence de l'Union qui a enregistré les données dans le système concerné. Pour ce faire, l'autorité en question devrait pouvoir avoir accès aux données stockées dans le CIR, le SIS et le MID (Paragraphe 42). L'unité centrale ETIAS a un droit d'accès aux « données pertinentes » du SIS. (Article 36 ter du règlement (UE) 2018/1861) L'interopérabilité* avec ETIAS est également prévue. (Article 36 quater du règlement (UE) 2018/1861) En vertu de l'article 15 du règlement (UE) 2018/1860, certaines données renseignées dans les signalements relatifs aux décisions de retour peuvent être transférées ou mises à disposition de pays dits tiers avec l'accord de l'État signalant, aux fins d'identification d'une personne ressortissante d'un pays dit tiers « *en séjour irrégulier et de la délivrance à celui-ci d'un document d'identification ou de voyage en vue de son retour* ».
Comment obtenir communication et rectification des données ?	Le droit d'opposition* n'est pas applicable au système national N-SIS. Les droits d'accès, de rectification et à l'effacement peuvent être exercés pour le SIS. Toutefois, un État membre peut décider de ne pas fournir les informations à la personne requérante si cela constitue une « mesure nécessaire et proportionnée » afin de : « *éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires* », « *éviter de*

	nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales », « *protéger la sécurité publique* », « *protéger la sécurité nationale* », « *protéger les droits et libertés d'autrui* ». (Article 53 du règlement (UE) 2018/1861) En France, les droits d'accès, de rectification, d'effacement et à la limitation des données s'exercent directement auprès du directeur général de la police nationale. Si une personne fait l'objet de restrictions de ces droits, elle doit s'adresser à la Commission nationale de l'informatique et des libertés. (Article R. 231-13 du code de la sécurité intérieure) Le groupe de coordination de contrôle du système d'information* Schengen II (SIS II GCC) a créé un guide pour l'exercice du droit d'accès, qui détaille les informations relatives aux droits d'accès, de rectification et d'effacement des données stockées dans le SIS.
Remarques	Le Comité de surveillance coordonnée, créé par le Contrôleur européen de la protection des données en 2018, est chargé de coordonner la surveillance du traitement des données à caractère personnel pour le système SIS. Son objectif est de s'assurer que les systèmes d'information à grande échelle des organes et agences de l'UE sont conformes à l'acte juridique qui les établit.
Textes qui régissent ce fichier	- Articles R. 231-1 à R. 231-16 du code de la sécurité intérieure - 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) - 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 de deuxième génération (SIS II) - Décret n° 2016-1956 du 28 décembre 2016 relatif à la partie nationale du système d'information Schengen de deuxième génération (N-SIS II) - Décret n° 2024-616 du 27 juin 2024 relatif à la partie nationale du système d'information Schengen - Liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d'information Schengen de deuxième génération, présentée conformément à l'article 31, paragraphe 8, du règlement (CE) no 1987/2006 du Parlement européen et du Conseil et à l'article 46, paragraphe 8, de la décision 2007/533/JAI du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information* Schengen de deuxième génération (2017/C 228/01) - 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 - 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 - 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 - Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité* des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil - Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité* des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 - Règlement (UE) 2021/1150 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) 2018/1862 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système européen d'information et d'autorisation concernant les voyages - Règlement (UE) 2021/1152 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) n° 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 et (UE) 2019/817 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système européen d'information et d'autorisation concernant les voyages - Règlement (UE) 2022/1190 du Parlement européen et du Conseil du 6 juillet 2022 modifiant le règlement (UE) 2018/1862 en ce qui concerne l'introduction dans le système d'information* Schengen (SIS) de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union
Sources	Barbou Des Places Ségolène, « 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 Cnil, « SIS II : Système d'information Schengen II » 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

	Commission européenne, « Signalements et données dans le SIS » European Data Protection Supervisor, « Système d'information Schengen (SIS) »

Nom du fichier	**VIS**
Sens de l'acronyme	Visa information system - Système d'information* sur les visas
Date de création	8 juin 2004
Quelle échelle ?	Européenne
Objectifs officiels	Le Système d'information* sur les visas (VIS) est utilisé pour l'examen des demandes de visas de court séjour, les visas de long séjour, les titres de 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 personnes demandeuses et détentrices de visa. Ses objectifs globaux sont l'amélioration de la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la possibilité de consultations entre les autorités centrales chargées des visas (EUR-Lex, 2023). Pour ce faire, le système VIS vise à : - Faciliter la procédure de demande de visa ; - Éviter les contournements des critères de détermination de l'État membre responsable de l'examen de la demande de visa ; - Faciliter la lutte contre la fraude ; - Faciliter les contrôles aux points de passage aux frontières extérieures et sur le territoire des États membres ; - Aider à l'identification de toute personne qui ne remplit pas ou plus les conditions d'entrée, de présence ou de séjour sur le territoire des États membres ; - Faciliter l'application du règlement (UE) n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (« Dublin III ») ; - Contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des États membres. (Article 2 du règlement (CE) n° 767/2008)
Objectif implicite	Le Visa Information System (VIS), qui centralise les données biométriques* des personnes détentrices de visa, fait partie des outils technologiques de surveillance mis en place à l'échelle européenne. Ces outils ont pour objectif de limiter la proportion de personnes étrangères sur le territoire après l'expiration de leur visa Schengen. Il vise aussi à empêcher que les personnes ressortissantes d'États dits tiers fassent plusieurs demandes de visa auprès de plusieurs services consulaires. (Barbou Des Places Ségolène, « 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) 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, *Visa Refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas*, Rapport d'observation, juillet 2010)
Contenu des données	Les catégories de données enregistrées dans le VIS sont : - Les données alphanumériques* sur la personne de demandeuse et sur les visas demandés, délivrés, refusés, annulés, retirés ou prorogés - Les photographies - Les empreintes digitales - Les liens avec les demandes de visa précédentes et avec les dossiers de demande des personnes qui voyagent ensemble - Un scan de la page des données biographiques du document de voyage L'ensemble des données est stocké dans le système central du VIS, à l'exception des nom, prénoms, date de naissance, sexe, lieu et pays de naissance, nationalité(s), type et numéro du ou des documents de voyage et pays de délivrance et date d'expiration de leur validité, de la photographie et des empreintes digitales de la personne demandeuse qui sont stockées dans le CIR. (Article 5 du règlement (CE) n° 767/2008) - Lorsqu'une demande est jugée recevable conformément au code communautaire 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)

	- 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 refuser 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)
Critères d'inscription dans ce fichier	Toute personne ayant fait une demande de visa pour entrer dans l'espace Schengen jugée recevable conformément au code communautaire des visas par les autorités consulaires.
Autorité(s) compétente(s)	Le système d'information* VIS est composé : - d'un système central, dont la gestion opérationnelle est effectuée par une instance gestionnaire, financée par le budget de l'Union Européenne, l'agence EU-Lisa ; - d'une infrastructure de communication entre le VIS principal et les interfaces nationales qui sont gérés par les autorités nationales. En France, le ministère de l'Europe et des affaires étrangères et le ministère de l'intérieur sont co-responsables du VIS. Le Comité de surveillance coordonnée, créé par le Contrôleur européen de la protection des données en 2018, est chargé de coordonner la surveillance du traitement des données à caractère personnel pour le système VIS. Son objectif est de s'assurer que les systèmes d'information à grande échelle des organes et agences de l'UE sont conformes à l'acte juridique qui les établit.
Qui a accès à ce fichier ?	Ont accès à ce fichier : - 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 du règlement (CE) n° 767/2008) ; - Autorités centrales chargées des visas pour les demandes de consultation, avec saisine du VIS central, qui transmet la demande aux États concernés (Article 16 du règlement (CE) n° 767/2008) ; elles peuvent consulter un ensemble de données pour établir des statistiques, sans identification du demandeur (Article 17 du règlement (CE) n° 767/2008) ; - 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 du règlement (CE) n° 767/2008) ; 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 du règlement (CE) n° 767/2008) ; - Autorités centrales chargées du contrôle sur le territoire (Article 19 du règlement (CE) n° 767/2008), pour vérifier l'identité du titulaire, l'authenticité du visa ou si les conditions d'entrée/de séjour sont remplies; 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 du règlement (CE) n° 767/2008) ; - Autorités compétentes en matière d'asile effectuant des recherches à l'aide des empreintes digitales pour deux motifs la consultation* du VIS étant autorisée pour ces autorités (Article 21 du règlement (CE) n° 767/2008) 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 États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JOUE L 218/129, 13 août 2008). En France, aucun service français ne dispose d'un accès direct* au VIS. Les échanges de données avec le système d'information* européen, ou la consultation* de ces informations, s'opèrent exclusivement par l'intermédiaire des applications informatiques nationales, c'est-à-dire traitements « Réseau mondial Visas 2 », « France-Visas » et « VISABIO ».

	Peuvent également accéder aux données à caractère personnel enregistrées dans le VIS, dans les conditions fixées à l'article L. 222-1 du code de la sécurité intérieure : - Les membres du personnel des services de la police nationale et les militaires des unités de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme, individuellement désignés et spécialement habilités respectivement par le directeur général dont ils relèvent ; - Les membres du personnel des services spécialisés du renseignement mentionnés à l'article R. 222-1 du code de la sécurité intérieure, individuellement désignés et spécialement 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 ; - À la seule fin d'effectuer les vérifications mentionnées au 7° de l'article R. 611-8, peuvent consulter les données relatives au nom, au prénom, à la date et au pays de naissance, à la photographie de l'étranger ainsi qu'à la délivrance d'un visa, à sa date, à sa durée de validité et aux documents de voyage le personnel des organismes de sécurité sociale individuellement désignés et spécialement habilités par les directeurs de ces organismes.
Durée de conservation des données	Chaque dossier de demande est enregistré dans le VIS pour une durée maximale de 5 ans. Seul le pays responsable est autorisé à modifier ou à supprimer les données qu'il a transmises au système VIS.
Échanges de données ?	En vertu du règlement (UE) 2019/817, l'ensemble des systèmes d'information de l'Union – soit l'EES, le VIS, l'ETIAS, EURODAC, le SIS II, l'ECRIS-TCN – doivent être interopérables. Les modalités de **connexion entre le VIS et l'EES** sont décrites aux articles 17 bis à 19 du règlement (CE) n°767/2008 (modifié par le règlement (UE) n°2023/2667). Un canal de communication sécurisé entre les deux systèmes doit être établi par l'EU-Lisa, et la consultation* directe entre l'EES et le VIS ne doit être possible que dans certaines conditions : - Les autorités chargées des visas utilisant le VIS peuvent consulter l'EES à partir du VIS : - Lors de l'examen des demandes de visa et des décisions y afférentes ; - Afin d'extraire et d'exporter directement du VIS vers l'EES les données relatives aux visas en cas d'annulation, de retrait ou de prorogation d'un visa. - Les autorités frontalières utilisant l'EES peuvent consulter le VIS à partir de l'EES afin : - D'extraire directement du VIS les données relatives aux visas et de les importer dans l'EES afin de permettre la création ou la mise à jour dans l'EES d'une fiche d'entrée/de sortie ou d'une fiche de refus d'entrée d'un titulaire de visa ; - D'extraire directement du VIS les données relatives aux visas et de les importer dans l'EES en cas d'annulation, de retrait ou de prorogation d'un visa ; - De vérifier l'authenticité et la validité du visa, le respect des conditions d'entrée sur le territoire des États membres ; - De vérifier si les personnes ressortissantes de pays dits tiers exemptées de l'obligation de visa pour lesquels aucun dossier individuel n'est enregistré dans l'EES étaient enregistrées précédemment dans le VIS ; - De vérifier, lorsque l'identité d'une personne titulaire de visa est vérifiée à l'aide des empreintes digitales, l'identité d'une personne titulaire de visa à l'aide de ses empreintes digitales par consultation* du VIS. Le service internet de l'EES, accessible aux personnes ressortissantes de pays dits tiers afin de vérifier la durée restante de leur séjour autorisé, est mis à jour quotidiennement via une extraction à sens unique « *des sous-ensembles minimaux nécessaires de données du VIS* ». (Article 17 bis du règlement (CE) n° 767/2008) « *L'extraction des données relatives aux visas depuis le VIS, leur exportation dans l'EES et la mise à jour des données du VIS dans l'EES constituent un processus automatisé une fois que l'opération en question est lancée par l'autorité concernée* ». (Article 17 bis) Dans le cadre des vérifications aux frontières auxquelles l'EES est mis en œuvre, les autorités compétentes ont accès au VIS pour effectuer des recherches à l'aide des données d'identité et relatives au(x) document(s) de voyage. Lorsqu'une recherche est lancée dans l'EES dans le cadre de ces recherches, l'autorité frontalière lance une recherche dans le VIS directement à partir de l'EES. Si la recherche montre que le VIS contient des données relatives à un ou plusieurs visas délivrés ou prorogés, en cours de validité temporelle et territoriale pour le franchissement des frontières, ou que le VIS contient des données mais qu'aucun visa valable n'est enregistré, l'autorité compétente peut consulter les données stockées dans le dossier en question, relatives au statut du visa et extraites du formulaire de demande, les photographies et les données ajoutées au dossier de la personne qui s'est vue délivrer un visa (listées à l'article 10), dont le visa a été annulé ou révoqué (listées à l'article 13) ou prorogé (listées à l'article 14). Par ailleurs, les autorités effectuant les contrôles aux frontières auxquelles l'EES est mis en œuvre peuvent vérifier l'identité d'une personne grâce au VIS si l'identité de la personne ne peut être vérifiée par consultation* de l'EES. Cette vérification se fait au moyen des empreintes digitales de la personne titulaire de visa ou des données alphanumériques* s'il est impossible d'utiliser les empreintes digitales (Article 18). Afin de créer ou mettre à jour une fiche de d'entrée / de sortie ou une fiche de refus d'entrée d'une personne titulaire de visa dans l'EES, l'autorité effectuant les vérifications aux frontières auxquelles l'EES est mis en œuvre est autorisée à extraire du VIS et à importer dans l'EES les données stockées dans le VIS citées à l'article 16, paragraphe 2 points c) à f) du règlement (UE) 2017/2226, relatives au statut de la personne, au visa de court séjour octroyé, à sa première entrée et la durée du séjour autorisé et la potentielle validité territoriale limité du visa de court séjour (Article 18 bis).

	En vertu des règlements n° 767/2008 et 2018/1240, le **système central ETIAS** pourra comparer certaines données avec les données stockées dans le VIS, notamment si la personne demandeuse d'une autorisation de voyage sur le territoire des États membres a fait l'objet d'une décision de refus, d'annulation ou de révocation d'un visa de court séjour (Article 20, paragraphe 2, point i) du règlement (UE) 2018/1240). Cette comparaison pourra s'effectuer via l'ESP et sera automatique. (Article 18 ter) Par ailleurs, l'unité centrale ETIAS pourra accéder aux données du VIS « pertinentes », aux fins de l'accomplissement de ses missions. (Article 18 quater) Les unités nationales ETIAS disposent d'un accès temporaire au VIS pour le consulter, en lecture seule, aux fins de l'examen des demandes d'autorisation de voyage. Le résultat de la consultation* est inscrit dans les dossiers de demande ETIAS. (Article 18 quinquies) Par ailleurs, le règlement (UE) 2019/817 crée le portail de recherche européen (**ESP**), qui comprend une infrastructure de communication sécurisée avec l'EES, le VIS, l'ETIAS, Eurodac, le SIS central, l'ECRIS-TCN, les données Europol et les bases de données d'Interpol, ainsi qu'avec les infrastructures centrales du CIR et du détecteur d'identités multiples (MID), également créé par le règlement (UE) 2019/817 (Article 6 du règlement (UE) 2019/817). Les autorités des États membres et agences de l'Union ayant accès à, au moins, l'un des systèmes d'information de l'UE peuvent utiliser l'ESP (Article 7 du règlement (UE) 2019/817). Ces autorités peuvent lancer une requête en soumettant les données alphanumériques* ou biométriques* à l'ESP. « *Lorsqu'une requête a été lancée, l'ESP interroge l'EES, ETIAS, le VIS, le SIS, Eurodac, l'ECRIS-TCN et le CIR ainsi que les données d'Europol et les bases de données d'Interpol, simultanément, à l'aide des données envoyées par l'utilisateur et conformément au profil d'utilisateur.* » Aucune information concernant des données à laquelle l'autorité lançant la requête n'a pas accès en vertu du droit de l'Union ne peut être communiquée par l'ESP. (Article 9 du règlement (UE) 2019/817) Le VIS est connecté au CIR, dans la mesure où lorsque des données sont ajoutées, modifiées ou supprimées dans le VIS, elles le sont également de manière automatique dans le dossier individuel du CIR. (Article 19 du règlement (UE) 2019/817) Lors de la création ou de la mise à jour d'un dossier de demande dans le VIS, les autorités chargées des visas peuvent avoir accès aux dossiers de confirmation d'identité stockés dans le MID aux fins de la vérification manuelle des différentes identités. (Article 26 du règlement (UE) 2019/817) Enfin, VISABIO est le fichier national français associé au fichier européen VIS. Aussi, le traitement VISABIO est connecté aux autorités des États Schengen au travers du système VIS. (Article R. 142-1 du CESEDA)
Comment obtenir communication et rectification des données ?	Les droits d'accès, de rectification, de modification et d'effacement s'appliquent et sont encadrés par l'article 38 du règlement (CE) n° 767/2008. En France, les droits d'accès et de rectification s'exercent 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). On peut également faire les démarches en se référant aux fichiers France-Visas et VISABIO.
Remarques	Il existe une possibilité d'externalisation des politiques migratoires, notamment à des acteurs privés : les communications de la DGEF du ministère de l'intérieur soulignent la volonté d'externaliser la gestion des visas et dans ce contexte le contrôle migratoire à des prestataires. Comme le note Statewatch, les modifications les plus récentes du règlement VIS, approuvées en juillet 2021, ajoutent des pouvoirs spécifiques aux membres des équipes Frontex pour utiliser le VIS aux fins de : Contrôles aux frontières, aux fins de « *vérification aux points de passage des frontières extérieures* » ; « *vérifier si les conditions d'entrée, de séjour ou de résidence sur le territoire des États membres sont remplies* » ; et Retour, pour « *identifier toute personne qui ne remplit pas ou ne remplit plus les conditions d'entrée, de séjour ou de résidence sur le territoire des États membres* ». Cet accès aux bases de données européennes à grande échelle permet aux membres des « équipes » Frontex d'effectuer des tâches de contrôle aux frontières ou d'expulsion. (Statewatch, *Frontex and the interoperable databases*, Rapport, 2024) Dans un autre rapport *Automating the fortress: digital technologies and European borders*, Statewatch remarque la potentialité d'intégrer des technologies algorithmiques et d'apprentissage automatique (machin learning) au système d'information* des visas donnant alors un rôle de contrôle. Ces technologies sont « destinées à détecter les individus potentiellement à risque pour les interroger davantage ou à les empêcher de voyager en premier lieu ».
Textes qui régissent ce fichier	- 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 - Décision du Conseil 2004/512/CE du 8 juin 2004 établissant le système d'information* sur les visas (VIS) - 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)

	- Règlement (CE) n° 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas - Règlements modifiant le règlement (CE) n° 767/2008 : Règlement (UE) n° 610/2013 du Parlement européen et du Conseil du 26 juin 2013 ; Règlement (UE) n° 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 ; Règlement (UE) n° 2019/817 du Parlement européen et du Conseil du 20 mai 2019 ; Règlement (UE) n° 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 ; Règlement (UE) n° 2021/1152 du Parlement européen et du Conseil du 7 juillet 2021 ; Règlement (UE) n° 2023/2667 du Parlement européen et du Conseil du 22 novembre 2023 - 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) - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) - Règlement (UE) 2024/1356 du Parlement européen et du Conseil du 14 mai 2024 établissant le filtrage des ressortissants de pays tiers aux frontières extérieures et modifiant les règlements (CE) n° 767/2008, (UE) 2017/2226, (UE) 2018/1240 et (UE) 2019/817
Source	Barbou Des Places Ségolène, « Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ? », *in Fichiers informatiques et sécurité publique*, Presse universitaire de Nancy, pp. 183 - 221, 2013 La Cimade, *Visa Refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas*, Rapport d'observation, juillet 2010 Comité européen de la protection des données, « Legal Framework - Coordinated Supervision Committee »EUR-Lex, « VIS regulation », 2023 Ministère de l'intérieur, « La biométrie et l'externalisation », 18 mars 2021 Migreurop, « Les visas : inégalités et mobilités à géométrie variable », novembre 2019 Statewatch, *Frontex and interoperable databases - Knowledge as power?*, Rapport, février 2023 Statewatch, *Automating the fortress: digital technologies and European borders*, Rapport, 6 juin 2024

Nom du fichier	**FIELDS**
Sens de l'acronyme	Frontex-INTERPOL Electronic Library Document System / Le Système Frontex-INTERPOL d'authentification de documents électroniques
Date de création	Mis en service en 2022
Quelle échelle ?	Internationale
Le système I-24/7	La base de données est accessible via le système mondial de communication policière I-24/7. Les pays membres échangent chaque année plus de 28 millions de messages de texte libre à l'aide de ce système. Les messages sont transmis et classés manuellement. Interpol a pour objectif de développer et de remplacer I-24/7 par un système de messagerie intelligent ayant recours à l'intelligence artificielle. (Interpol, Le système de messagerie intelligent)
Objectifs officiels	Le Système Frontex-INTERPOL d'authentification de documents électroniques (FIELDS) donne aux policiers et aux garde-frontières des informations visuelles sur les principaux éléments susceptibles d'indiquer qu'un document est contrefait ou falsifié. Le fichier FIELDS permet, selon le site d'Interpol, de : - Assurer une utilisation rationnelle et durable du système (sur le plan opérationnel et technique) ; - Étendre le système aux infrastructures nationales de sécurité aux frontières de tous les pays membres d'INTERPOL ; - Améliorer les procédures opérationnelles et techniques. Sur le terrain, le FIELDS est utilisé en première ligne des contrôles aux frontières. Il serait utilisé avec les fiches de vérification rapide créées par Frontex et permettra de vérifier rapidement les documents falsifiés. La fiche de vérification rapide est une aide à la décision visuelle. Elle propose un modèle du document qui fait l'objet de la vérification et fait apparaître les principaux éléments de sécurité à vérifier. Les personnes dont les documents sont signalés devront effectuer un contrôle de seconde ligne.
Objectif implicite	Empêcher la circulation des personnes dont on considère leur document frauduleux, ou établi frauduleux par le FIELDS et les autorités de contrôle.
Contenu des données	Elle associe une version de la plateforme Dial-Doc[36] (bibliothèque numérique d'Interpol d'alerte sur les documents de voyage) existante d'INTERPOL avec les fiches de vérification rapide de Frontex, pour les mettre à la disposition des agents chargés des contrôles aux frontières via le système mondial de communication policière sécurisée I-24/7 d'INTERPOL. L'objectif est d'intégrer à cette base de données de nouvelles fonctionnalités comme l'intelligence artificielle, l'automatisation. (Interpol, FIELDS Database-Project, 2022)
Critères d'inscription dans ce fichier	Information non disponible
Autorité(s) compétente(s)	Interpol
Qui a accès à ce fichier ?	- Les Bureaux centraux nationaux - Les entités nationales - Les entités internationales - Le personnel de contrôle aux frontières de Frontex
Durée de conservation des données	Information non disponible
Échanges de données avec d'autres fichiers ?	Selon la communication de Frontex : le FIELDS permet « *de consulter des ensembles de données relatives aux documents* ». Selon Interpol : « *les informations relatives aux contrefaçons et aux falsifications proposées par le système FIELDS viennent compléter celles de la base de données SLTD existante d'INTERPOL, qui contient des informations sur les documents volés, perdus, révoqués, invalides ou volés vierges.* »
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.* »

[36] La plateforme Dial-Doc est une technologie de vérification des documents de voyage en le comparant avec des images de documents (Voir Interpol, INTERPOL met en service une nouvelle technologie pour détecter les documents de voyage frauduleux).

	(Article 18 du règlement d'Interpol sur le traitement des données) En France il est possible de s'adresser à la Commission de contrôle des fichiers d'Interpol (200 quai Charles de Gaulle, 69006 Lyon) pour demander l'accès, la rectification et l'effacement des données. (Article 18 du règlement sur le traitement des données d'Interpol, et règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol) **Il existe un guide de procédure à l'intention des demandeurs et demandeuses qui saisissent la Commission.** (CCF Procedural guidelines for applicants FR)
Remarques	Pas de document législatif accessible. Dans la communication d'Interpol, on peut lire : « *Dans l'avenir, l'unité FIELDS travaillera à intégrer de nouvelles fonctionnalités telles que l'intelligence artificielle et la compatibilité avec les postes de contrôle frontalier automatisé. Pour atteindre ces objectifs et alimenter la base de données avec autant d'informations utiles que possible, INTERPOL et Frontex resteront tributaires de leurs pays membres en ce qui concerne l'échange de spécimens de documents et d'informations connexes. L'unité FIELDS sera basée à INTERPOL et bénéficiera de l'expertise et du financement de Frontex, témoignant de leur volonté commune d'élargir la palette des outils de gestion des frontières mis à la disposition des agents de première ligne et de renforcer la sécurité mondiale.* » Ainsi, Frontex finance et a accès au FIELDS mais n'est pas responsable du traitement.
Textes 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. Règlement disponible sur le site d'Interpol, rubrique « Documents juridiques » - Statut d'Interpol I/CONS/GA/1956 du 13 juin 1956, disponible sur le site d'Interpol, rubrique « Documents juridiques »
Sources	Site d'Interpol, voir les différentes rubriques citées ci-dessus JurisClasseur Droit international, Fasc. 409-10 : « ENTRAIDE JUDICIAIRE INTERNATIONALE. – Organisation internationale de police criminelle – Interpol », 15 juin 2018 Base de données FIELDS

Nom du fichier INTERPOL	**SLTD**
Sens de l'acronyme	Stolen and Lost Travel Documents / Fichier des documents de voyages et d'identité perdus ou volés
Date de création	2002
Quelle échelle ?	Internationale
Le système I-24/7	La base de données est accessible via le système mondial de communication policière I-24/7. Les pays membres échangent chaque année plus de 28 millions de messages de texte libre à l'aide de ce système. Les messages sont transmis et classés manuellement. Interpol a pour objectif de développer et de remplacer I-24/7 par un système de messagerie intelligent ayant recours à l'intelligence artificielle. (Interpol, le système de messagerie intelligent)
Objectifs officiels	Le fichier SLDT permet, selon le site d'Interpol, de : - Contrôler la validité d'un document de voyage ou d'identité en quelques secondes ; - Identifier et empêcher les criminels d'utiliser des documents de voyage perdus ou volés bien avant qu'ils ne se rendent à l'aéroport ou à la frontière.
Objectif implicite	Surveillance accrue et limitation de la circulation des personnes étrangères.
Contenu des données	Information non disponible
Critères d'inscription dans ce fichier	Avoir un document de voyage et d'identité déclarés volés, perdus, révoqués, invalides ou volés vierges.
Autorité(s) compétente(s)	Les Bureaux centraux nationaux et le Secrétariat général. Les pays alimentent la base de données en y enregistrant les documents de voyage et d'identité déclarés volés, perdus, révoqués, invalides ou volés vierges. Seul le pays ayant délivré le document peut l'ajouter dans la base de données, par l'intermédiaire de son Bureau central national INTERPOL ou des services chargés de l'application de la loi habilités à cette fin.
Qui a accès à ce fichier ?	- Les Bureaux centraux nationaux d'Interpol peuvent ajouter les documents de voyage d'identité perdus ou volés. Seuls eux peuvent enregistrer les documents de voyages sur la base de données. - Les entités nationales - Les entités internationales - Les personnels chargés de l'application de la loi affectés aux Bureaux centraux nationaux et sur le terrain dans les aéroports ou aux frontières - Les partenaires du secteur privé d'Interpol qui peuvent contrôler, à l'aide de la base de données sur les SLTD, les documents de voyage présentés par les clients achetant des titres de transport. Tout signalement positif sera communiqué aux services chargés de l'application de la loi, qui prendront les mesures nécessaires. (Par exemple Uber, Western Union : voir Partenariats)

Durée de conservation des données	- 5 ans pour les documents volés, perdus, révoqués ou invalides - 30 ans pour les documents volés vierges ou durée de conservation inférieure fixée par la source ou lorsque la finalité est atteinte
Échanges de données avec d'autres fichiers ?	Par le **portail de recherche européen (ESP)**, sont interrogés simultanément le SLTD, TDWAN, EES, VIS, ETIAS, EURODAC, SIS II et l'ECRIS-TCN. « *Le système central ETIAS lance une recherche en utilisant l'ESP [portail de recherche européen] pour comparer les données pertinentes [et] figurant dans un relevé, un dossier ou un signalement enregistré dans un dossier de demande stocké dans le système central ETIAS, le SIS, l'EES, le VIS, Eurodac, les données d'Europol et dans les bases de données SLTD et TDAWN d'Interpol.* » (Article 61, paragraphe 8 du règlement (UE) 2019/817) Les utilisateurs de l'ESP lancent une requête en soumettant des données alphanumériques* ou biométriques* à l'ESP. Interconnexion également avec le fichier API-PNR (cf Cnil, « Le système API-PNR France », 10 août 2016). **En France, le fichier SLDT d'Interpol est notamment interconnecté avec le fichier TES, DOCVERIF, FAED** (Caisse de solidarité de Lyon, « La folle volonté de tout contrôler », avril 2024)
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) En France il est possible de s'adresser à la Commission de contrôle des fichiers d'Interpol (200 quai Charles de Gaulle, 69006 Lyon) pour demander l'accès, la rectification et l'effacement des données (Article 18 du règlement sur le traitement des données d'Interpol, et règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol). **Il existe un guide de procédure à l'intention des demandeurs qui saisissent la Commission.** (CCF Procedural guidelines for applicants FR)
Remarques	La base de données SLTD comprend actuellement environ 128 millions d'enregistrements. 3,6 milliards de recherches ont été effectuées dans la base en 2023 et ont donné lieu à 232 423 signalements positifs (ou hits). Voir Base de données SLTD (documents de voyage et d'identité) Interpol
Textes 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. Règlement disponible sur le site d'Interpol, rubrique « Documents juridiques » - Statut d'Interpol I/CONS/GA/1956 du 13 juin 1956, disponible sur le site d'Interpol, rubrique « Documents juridiques »
Sources	Site d'Interpol, voir les différentes rubriques citées ci-dessus JurisClasseur Droit international, Fasc. 409-10 : « ENTRAIDE JUDICIAIRE INTERNATIONALE. – Organisation internationale de police criminelle – Interpol », 15 juin 2018 Base de données SLTD (documents de voyage et d'identité) Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024

Nom du fichier	**EUROPOL**
Sens de l'acronyme	European police office / Agence de l'Union européenne pour la coopération des services répressifs
Date de création	26 juillet 1995
Quelle échelle ?	Européenne et internationale
Objectifs officiels	Europol est une agence de l'UE destinée à faciliter la coopération policière européenne et responsable en dernier ressort devant le Conseil des ministres de la Justice et des Affaires intérieures, qui comprend les ministères compétents de tous les États membres de l'UE. Le Conseil de l'UE est responsable du contrôle et de l'orientation d'Europol et nomme le personnel de direction exécutif et le personnel de direction adjoint de l'agence. Dès l'origine, ses objectifs sont notamment la collecte, l'analyse et l'échange d'informations entre les États européens, et la gestion de données. Les données à caractère personnel sont également collectées et traitées à des fins d'analyses de nature stratégique ou thématique, d'analyses opérationnelles ou de facilitation de l'échange d'informations entre les États membres, Europol, d'autres organes de l'Union, des pays tiers et des organisations internationales. (Voir 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) « *Compte tenu de l'implication d'Europol dans la surveillance des technologies émergentes, ainsi que de sa participation à l'élaboration de nouvelles façons d'utiliser ces technologies à des fins répressives, notamment par l'intermédiaire de son laboratoire d'innovation et du pôle d'innovation de l'Union européenne pour la sécurité intérieure, Europol possède une très bonne connaissance des possibilités offertes par ces technologies ainsi que des risques liés à leur utilisation. Elle devrait donc pouvoir soutenir les États membres dans le filtrage des investissements directs étrangers dans l'Union et des risques connexes pour la sécurité qui concernent des entreprises qui fournissent des technologies, y compris des logiciels, utilisées par Europol aux fins de la prévention des formes de criminalité qui relèvent des objectifs d'Europol et des enquêtes en la matière, ou encore des technologies critiques qui pourraient être utilisées pour faciliter des actes terroristes. Dans ce contexte, l'expertise d'Europol devrait venir en appui du filtrage des investissements directs étrangers et des risques connexes pour la sécurité. Il convient de tenir compte en particulier de la question de savoir si l'investisseur étranger a déjà participé à des activités portant atteinte à la sécurité, s'il existe un risque grave que l'investisseur étranger se livre à des activités illégales ou criminelles, et si celui-ci est contrôlé directement ou indirectement par le gouvernement d'un pays tiers, y compris au moyen de subventions*. » (Paragraphe 13 du préambule du règlement (UE) 2022/991) Définis dans l'article 4 du 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), ses objectifs sont de : - Composition : regroupe les services de police et les douanes des États membres. Chaque État membre met en place une unité nationale (au sein de laquelle au moins une officière ou un officier de liaison est désigné) constituant l'organe de liaison entre Europol et les autorités compétentes de l'État membre. Europol dispose également de personnels de liaisons. - Mission : faciliter l'échange d'informations, les analyser et coordonner les opérations entre les États membres de l'Union européenne pour lutter contre la criminalité internationale, le terrorisme et l'immigration clandestine. (Voir l'ensemble des missions à l'article 4 du règlement (UE) 2016/794) Europol n'est pas à proprement parler une police européenne car elle 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, elle emploie en revanche des officiers ou officières de liaisons (OLE) détachées auprès de l'agence par les États membres, qui coordonnent et centralisent les enquêtes.
Objectifs implicites	« *Les attributions d'Europol sont largement plus développées que celles qui étaient prévues à l'origine […] et intègrent notamment la lutte contre les filières d'immigration* [dites par les institutions] *clandestine*. » (Sylvia Preuss-Laussinotte, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, 2000). Le fichier d'Europol participe ainsi aux contrôles des frontières des États-membre de l'UE. Plusieurs associations, dont Statewatch, démontrent qu'Europol participe à la criminalisation des personnes en migrations et de leur soutien. (#Protectnotsurveil, Stopping the unfettered expansion of europol's digital surveillance powers against migrants, 2025)
Contenu des données	Les renseignements d'état civil : - Nom actuel et noms précédents ; prénom actuel et prénoms précédents ; nom de jeune fille ; nom et prénom du père (si nécessaire à des fins d'identification) ; nom et prénom de la mère (si nécessaire à des fins d'identification) ; sexe ; date de naissance ; lieu de naissance ; nationalité ; situation de famille ; pseudonymes ; surnom ; noms d'emprunt ou faux noms ; résidence et/ou domicile actuels et antérieurs Description physique :

	- Signalement physique ; signes particuliers (marques, cicatrices, tatouages, etc.) - Moyens d'identification : documents d'identité/permis de conduire ; numéros de la carte d'identité nationale/du passeport ; numéro d'identification national/numéro de sécurité sociale, le cas échéant - Représentations visuelles et autres informations concernant l'aspect extérieur ; informations permettant l'identification médico-légale, telles qu'empreintes digitales, profil ADN (établi à partir de l'ADN non codant), empreinte vocale, groupe sanguin, dossier dentaire - Profession et qualifications - Informations d'ordre économique et financier Informations relatives au comportement : - Mode de vie (par exemple, train de vie sans rapport avec les revenus) et habitudes ; déplacements ; lieux fréquentés ; armes et autres instruments dangereux ; degré de dangerosité ; risques particuliers, tels que probabilité de fuite, utilisation d'agents doubles, liens avec des membres de services répressifs ; traits de caractère ayant un rapport avec la criminalité ; toxicomanie - Contacts et entourage, y compris type et nature du contact ou de la relation - Moyens de communication utilisés, tels que téléphone (fixe/mobile), télécopieur, messagerie, courrier électronique, adresses postales, connexion(s) sur l'internet - Moyens de transport utilisés tels que véhicules automobiles, embarcations, avions, avec indication de leurs éléments d'identification (numéros d'immatriculation) Informations relatives aux activités criminelles : - Les infractions pénales et infractions pénales présumées, avec leurs dates, lieux et modalités ; les moyens utilisés ou susceptibles d'avoir été utilisés pour commettre ces infractions pénales, y compris les informations relatives aux personnes morales ; les services traitant l'affaire et leurs numéros de dossiers ; la suspicion d'appartenance à une organisation criminelle ; les condamnations, si elles concernent des infractions pénales relevant de la compétence d'Europol ; la personne introduisant les données. (Voir liste détaillée à l'annexe II du règlement n° 2016/794)
Critères d'inscription dans ce fichier	- Personnes qui sont soupçonnées d'avoir commis une infraction pénale ou d'avoir participé à une infraction pénale relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction - Personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire pour Europol et les États membres d'Europol qu'elles commettront des infractions pénales relevant de la compétence d'Europol (Article 8 de l'Europol Act 2012, et l'article 18 du règlement (UE) 2016/794)
Autorité(s) compétente(s)	Europol Le Comité de surveillance coordonnée, créé par le Contrôleur européen de la protection des données en 2018, est chargé de coordonner la surveillance du traitement des données à caractère personnel par Europol. Son objectif est de s'assurer que les systèmes d'information à grande échelle des organes et agences de l'UE sont conformes à l'acte juridique qui les établit.
Qui a accès à ce fichier ?	Le fichier Europol est alimenté par les États membres, via l'unité nationale de contact avec Europol présente dans chaque État membre. Les États-membre de l'UE (Article 20 du règlement UE 2016/794) **Les États membres d'Europol** (Article 20 du règlement UE 2016/794) Les membres du personnel d'Europol dûment habilités par le directeur exécutif (Article 20 du règlement précité) **Eurojust**[37]et l'Office européen de lutte antifraude (OLAF), dans le cadre de leurs mandats respectifs peuvent disposer d'un accès indirect* aux informations fournies à Europol (Article 21 du règlement précité)
Durée de conservation des données	Les données sont conservées « 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 3 ans après le début de leur traitement initial. Lorsqu'un État transmet des données à Europol, il peut définir un délai au-delà duquel elles sont effacées (Article 19 du règlement 2016/794). Si l'État qui a fourni les informations a indiqué un tel délai au-delà duquel elles doivent être effacées, à l'issue de ce délai, Europol peut demander à cet État l'autorisation de continuer à les conserver. De la même manière, l'État qui efface des données dans ses fichiers nationaux doit en informer Europol, qui les efface à son tour, sauf s'il demande à cet État l'autorisation de les conserver. (Article 31 du règlement UE 2016/794)

[37] Eurojust est l'agence européenne chargée de renforcer la coopération judiciaire entre les États membres, pour les poursuites relatives à la criminalité organisée.

Échange de données	Europol a accès aux données du SIS II et du VIS. 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. Ainsi qu'avec les États membres d'Europol : le Royaume-Uni (Accord de septembre 2021), la Géorgie (Accord du 4 avril 2017), le Liechtenstein (Accord du 7 juin 2013), Monaco (Accord du 6 mai 2011), l'Ukraine (Accord du 14 décembre 2016), la Bosnie Herzégovine (Accord du 31 août 2016), les États-Unis (Accord du 20 décembre 2002), la Serbie (Accord du 16 janvier 2014), la Norvège (Accord du 28 juin 2001), le Monténégro (Accord du 29 septembre 2014), la Moldavie (Accord du 18 décembre 2014), la Macédoine (2007), l'Islande, la Colombie, le Canada (Accord du 21 novembre 2005), l'Australie (Accord du 20 février 2007), l'Albanie (Accord du 9 décembre 2013) et la Suisse (Accord du 24 septembre 2004).
Comment obtenir communication et rectification des données ?	L'article 36 du règlement prévoit que les personnes concernées peuvent demander l'accès aux informations qui les concernent sont traitées par Europol. Elles peuvent s'adresser aux autorités de l'État de leur choix, qui fait suivre à Europol sous le délai d'un mois. En France, il faut s'adresser à la Cnil, à la direction générale de la police nationale ou à la direction générale de la gendarmerie nationale. Europol doit répondre dans un délai de 3 mois à compter de la réception de la demande. Europol, avant de donner l'accès aux données à la personne concernée, interroge les États membres, qui peuvent s'opposer à la transmission des informations. En cas de refus, la personne en est informée par Europol. Europol peut aussi décider d'informer la personne uniquement du fait qu'il a effectué les vérifications nécessaires. La personne peut introduire un recours devant le Centre européen de protection des données, rue Wiertz 60, B-1047 Bruxelles, BELGIQUE. L'article 37 du règlement prévoit qu'une personne peut aussi demander la limitation du traitement (la conservation des données détenues par Europol pour qu'elle puisse s'en servir comme preuve), la rectification et l'effacement des données la concernant. Elle peut s'adresser à l'État de son choix (en France, ça doit être la Cnil, la direction générale de la police nationale ou à la direction générale de la gendarmerie nationale). Pour la rectification et l'effacement, la personne doit avoir eu préalablement accès aux données la concernant. La réponse d'Europol doit intervenir sous 4 mois. En cas de refus, la personne concernée peut introduire un recours devant le Centre européen de protection des données, rue Wiertz 60, B-1047 Bruxelles, BELGIQUE. Selon la Caisse de solidarité de Lyon dans La folle volonté de tout contrôler : « *Si la procédure ouverte à l'égard de la personne concernée est définitivement classée ou si cette personne est définitivement acquittée, les données relatives à l'affaire ayant fait l'objet de cette décision sont effacées* ».
Remarques	Les nombreux accords de coopération signés par Europol avec des pays tiers, des organisations internationales et d'autres agences européennes (comme FRONTEX) ont 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. (Sylvia Preuss-Laussinotte, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », 2009)
Textes qui régissent ce fichier	- Europol Act du 26 décembre 2012 - 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 modifié par le règlement (UE) 2022/991 - Règlement (UE) 2022/991 du Parlement européen et du Conseil du 8 juin 2022 modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données* à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation
Sources	Site de EUR-Lex, voir ci-dessus les « Textes qui régissent ce fichier » Caisse de solidarité de Lyon, « La folle volonté de tout contrôler - Les fichiers d'identification administrative, de police, de justice et de renseignement : Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression », avril 2024 European Data Protection Board Preuss-Laussinotte Sylvia, *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité*, LGDJ, Bibliothèque de droit public, 2000 Preuss-Laussinotte Sylvia, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*, n° 74, p. 81-90, été 2009 #Protectnotsurveil, Stopping the unfettered expansion of europol's digital surveillance powers against migrants, 2025

Nom	**FRONTEX**
Sens de l'acronyme	The European Border and Coast Guard Agency / Agence européenne de garde-frontières et de garde-côtes
Date de création	2004
Quelle échelle ?	Européenne
Objectifs officiels	Frontex est l'agence européenne de garde-frontières et de garde-côtes ayant pour objectif : - « *Le soutien des États-membres de l'UE et des pays associés à l'espace Schengen dans la gestion des frontières extérieures de l'UE* - *La lutte contre la criminalité transfrontalière* » L'Agence est responsable devant le Parlement européen et le Conseil. (Frontex, « Qui sommes-nous », 2025) Ses missions sont : - « *de surveiller les flux migratoires et d'effectuer une analyse des risques en ce qui concerne tous les aspects de la gestion intégrée des frontières* - *d'assurer le suivi des besoins opérationnels des États membres en ce qui concerne la mise en œuvre des retours, y compris en recueillant des données opérationnelles* - *de procéder à des évaluations de la vulnérabilité, y compris des évaluations de la capacité et de l'état de préparation des États membres pour faire face aux menaces et aux problèmes qui se posent aux frontières extérieures* - *d'assurer le suivi de la gestion des frontières extérieures par l'intermédiaire des officiers de liaison de l'Agence dans les États membres* - *de contrôler le respect des droits fondamentaux dans l'ensemble de ses activités, aux frontières extérieures et dans les opérations de retour* - *de soutenir l'élaboration et la gestion d'EUROSUR* - *d'apporter une assistance technique et opérationnelle aux États membres et aux pays tiers* - *de déployer le contingent permanent dans le cadre des équipes affectées à la gestion des frontières, des équipes d'appui à la gestion des flux migratoires et des équipes affectées aux opérations de retour (collectivement dénommées «équipes») lors d'opérations conjointes ainsi que pour des interventions rapides aux frontières, des opérations de retour et des interventions en matière de retour* - *de constituer un parc des équipements techniques, comprenant un parc d'équipements de réaction rapide, destinés à être déployés lors d'opérations conjointes, d'interventions rapides aux frontières et dans le cadre d'équipes d'appui à la gestion des flux migratoires, ainsi que pour des opérations de retour et des interventions en matière de retour* - *de constituer une réserve de contrôleurs des retours forcés* - *de déployer des équipes affectées aux opérations de retour pendant les interventions en matière de retour* - *de coopérer avec la FRA, dans les limites de leur mandat respectif, afin d'assurer l'application continue et uniforme de l'acquis de l'Union en matière de droits fondamentaux; avec l'Agence européenne de contrôle des pêches (AECP) et l'Agence européenne pour la sécurité maritime (AESM), dans les limites de leur mandat respectif, afin de soutenir les autorités nationales exerçant des fonctions de garde-côtes définies à l'article 69, y compris le sauvetage de personnes en mer, en fournissant des services, des informations, des équipements et des formations, ainsi qu'en coordonnant des opérations polyvalentes* - *de coopérer avec les pays tiers en ce qui concerne les domaines relevant du présent règlement, y compris par le déploiement opérationnel éventuel d'équipes affectées à la gestion des frontières dans les pays tiers* - *d'assister les États membres et les pays tiers dans le contexte de la coopération technique et opérationnelle entre eux dans les domaines couverts par le présent règlement* - *d'assister les États membres et les pays tiers pour la formation des garde-frontières, des autres agents compétents et des experts nationaux en matière de retour, y compris par la définition de normes et de programmes de formation communs, notamment en matière de droits fondamentaux* - *de participer à l'évolution et à la gestion des activités de recherche et d'innovation présentant de l'intérêt pour le contrôle des frontières extérieures, y compris l'utilisation d'une technologie de surveillance avancée, et d'élaborer des projets pilotes propres lorsque cela est nécessaire à la mise en œuvre des activités prévues par le présent règlement* - *de développer des normes techniques applicables aux échanges d'informations* - *d'élaborer et d'exploiter, conformément au règlement (UE) 2018/1725, des systèmes d'information permettant des échanges rapides et fiables d'informations relatives aux risques émergents dans le cadre de la gestion des frontières extérieures, à l'immigration illégale et au retour, en étroite coopération avec la Commission, les organes et organismes de l'Union ainsi que le réseau européen des migrations établi par la décision 2008/381/CE du Conseil* »

	(Voir le détail et l'ensemble des missions à l'article 10 du règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes)
Objectif implicite	Frontex participe à la généralisation du fichage des personnes en migration au détriment du respect de leurs droits et à des fins de tri, de contrôle, d'enfermement et d'expulsions. Comme le rappelle StateWatch, Frontex « *est à la fois politiquement engagé et légalement obligé de garantir l'utilisation de technologies de pointe pour la surveillance et le contrôle des frontières* ». Elle joue un rôle dans l'influence des priorités de recherche de l'UE en matière de sécurité, notamment en parrainant et/ou commandant des recherches sur les nouvelles technologies pour les contrôles aux frontières. Frontex dispose d'un accès opérationnel et statistique aux bases de données de l'UE. « *L'accès à de vastes bases de données de l'UE permet aux membres des « équipes » de Frontex d'effectuer des tâches de contrôle des frontières ou d'expulsion : par exemple, vérifier la validité du visa d'une personne à un passage frontalier (système d'information sur les visas) ou établir si un avis d'éloignement a été émis à l'encontre d'une personne par les autorités nationales (système d'information Schengen).* » « *En 2019, alors même que rien ne le justifie, une troisième révision de son mandat renforce à nouveau les moyens financiers, techniques et humains de l'agence (corps permanent de 10 000 garde-frontières d'ici 2027). Ses pouvoirs en matière d'expulsions sont accrus et certains de ses pouvoirs d'exécution étendus pour s'assimiler à ceux des garde-frontières nationaux. Si l'agence peut autoriser ou non l'entrée à la frontière de l'UE, elle ne peut, en théorie, délivrer de laissez-passer européens qui restent de la compétence des États-membres, également responsables du bien-fondé de la décision de retour. Si Frontex ne peut préparer les décisions d'expulsion, elle voit son rôle renforcé dans l'identification des personnes faisant l'objet d'une mesure d'expulsion, la collecte des informations nécessaires à la mise en œuvre effective des expulsions et l'obtention des documents de voyage auprès des autorités consulaires des pays de renvoi, sans plus de détails sur ce que cela suppose. Enfin, seront désormais présents sur l'ensemble des vols conjoints d'expulsion des « contrôleurs des droits fondamentaux », nouvelles figures censément indépendantes (même si statutairement intégrées à Frontex), qui s'ajoutent ou se substituent aux contrôleurs des retours, rattachés à l'agence* ». (Gisti, « Frontex, l'agence européenne d'expulsion », in Plein droit, 2020) L'accès statistique permet à Frontex d'établir des « analyses de risques ». « *Loin de se cantonner à la centralisation des informations qu'elle recueille, l'agence joue un rôle actif de production d'informations. Les données collectées et exploitées, selon des processus opaques, nourrissent des analyses de risque sur le « crime transfrontalier » qui n'hésitent pas à faire le lien entre « franchissement irrégulier des frontières » et risque terroriste, sans preuve aucune. Les rapports servent ensuite de source majeure pour l'élaboration des politiques migratoires* ». (Migreurop, Frontex, une agence européenne hors de contrôle, Note, 2021)
Contenu des données	Frontex dispose d'un accès aux fichiers de l'UE : API-PNR, CIR, ECRIS-TCN, EES, ETIAS, EURODAC, SIS II, VIS. Frontex assure la création et le fonctionnement de l'unité centrale d'ETIAS. Durant les opérations conjointes, les opérations de retour, les interventions en matière de retour, les projets pilotes, les interventions rapides aux frontières et les déploiements des équipes d'appui à la gestion des flux migratoires, Frontex collecte : - « *les données à caractère personnel de personnes qui franchissent les frontières extérieures sans autorisation ;* - *les données à caractère personnel qui sont nécessaires pour confirmer l'identité et la nationalité des ressortissants de pays tiers dans le cadre des activités liées au retour, y compris les listes de passagers* - *les numéros de plaques d'immatriculation, les numéros d'identification de véhicules, les numéros de téléphone ou les numéros d'identification de navires et d'aéronefs qui sont liés aux personnes visées au point a) et qui sont nécessaires pour analyser les itinéraires et les méthodes utilisés pour l'immigration illégale.* » (Article 88 du règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes) Dans le cadre du traitement de données relatif au mécanisme de supervision de l'usage de la force par les officiers du corps permanent et les membres déployés des équipes : - nom, prénom, date de naissance, lieu de naissance, - détails du document, - informations sur les dommages corporels, - informations sur d'autres dommages Dans le cadre du traitement de données relatif au système de surveillance des retours forcés (SGRF) : - « *le sexe, l'âge, la nationalité,* - *le numéro de siège,*

	- *les détails de l'incident,* - *mesures coercitives appliquées, etc.* » (Frontex, « Protection des données ») Dans le cadre du traitement des données opérationnelles à caractère personnel, Frontex peut collecter : - les numéros des plaques d'immatriculation, les numéros d'identification des véhicules, les numéros de téléphone, les numéros d'identification de navires ou d'aéronefs liés à des personnes physiques dont les autorités compétentes des États membres, Europol, Eurojust ou Frontex ont des motifs raisonnables de soupçonner l'implication dans des activités criminelles trans frontalières ; - Ces données à caractère personnel peuvent comprendre des données à caractère personnel de victimes ou de témoins lorsque ces données à caractère personnel complètent les données à caractère personnel de suspects traitées par l'Agence. (Article 90 du règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes)
Autorité(s) compétente(s)	Un ou une déléguée à la protection des données est nommé au sein de Frontex. Le ou la Contrôleuse de la protection des données européennes de l'UE a également accès aux opérations de traitement des données à caractère personnel.
Qui a accès à ce fichier ?	Les agents et agentes de Frontex. « La collecte de données personnelles sur le terrain lors des entretiens avec les migrants (la principale source de données de Frontex lors des opérations conjointes) présente différents problèmes, tels que la nature non volontaire des entretiens et le manque de protection de l'identité des personnes interrogées. En outre, l'organisme a constaté que Frontex partageait directement les rapports de débriefing avec d'autres agences répressives de l'UE — l'Agence de l'UE pour la coopération des services répressifs (Europol) et l'Agence de l'UE pour la coopération judiciaire en matière pénale (Eurojust) — et les autorités des États membres sans évaluer la nécessité d'un tel partage. Cette pratique enfreint la législation européenne, affirme le CEPD, qui a ouvert une enquête sur le sujet en juin dernier » (Euractiv, « Frontex : le Contrôleur européen de la protection des données tire la sonnette d'alarme sur le traitement des données des migrants », 2023)
Durée de conservation des données	Frontex doit supprimer les données à caractère personnel dès qu'elles ont été transmises aux autorités compétentes des États membres, à d'autres organes et organismes de l'Union, en particulier à l'EASO, ou transférées vers des pays tiers ou à des organisations internationales, ou utilisées pour la préparation d'analyses des risques. La durée de conservation des données n'excède en aucun cas 90 jours après la date à laquelle elles ont été recueillies. Les données à caractère personnel traitées aux fins de l'accomplissement des tâches liées au retour sont supprimées dès que la finalité pour laquelle elles ont été recueillies a été atteinte et au plus tard trente jours après la fin de ces tâches. Les données opérationnelles à caractère personnel traitées aux fins de l'article 90 sont supprimées dès que la finalité pour laquelle elles ont été recueillies a été atteinte par l'Agence. L'Agence réexamine en permanence la nécessité de conserver ces données, en particulier les données à caractère personnel des victimes et des témoins. En tout état de cause, l'Agence réexamine la nécessité de conserver ces données au plus tard 3 mois après le début de leur traitement initial, et tous les 6 mois par la suite. (Article 91 règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes) Dans le cadre du traitement de données relatif au mécanisme de supervision de l'usage de la force par les officiers du corps permanent et les membres déployés des équipes pendant 5 ans à compter de l'enregistrement des données. Dans le cadre du traitement de données relatif au système de surveillance des retours forcés (SGRF), les données sont conservées pendant 5 ans.
Échanges de données avec d'autres fichiers ?	Dans le cadre du « traitement des données opérationnelles à caractère personnel », Frontex peut échanger des données avec : - « *Europol ou Eurojust, lorsque ces données sont strictement nécessaires pour l'exécution de leur mandat respectif et conformément à l'article 68* - *les autorités répressives compétentes des États membres, lorsque ces données sont strictement nécessaires pour ces autorités à des fins de prévention ou de détection de formes graves de criminalité transfrontalière et d'enquêtes ou de poursuites en la matière.* » (Article 90 du règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes)
Textes qui régissent ce fichier	- Règlement (UE) 2016/1624 du parlement européen et du conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du parlement européen et du Conseil et abrogeant le règlement (CE) n°2007/2004 Parlement européen et du Conseil, le règlement (CE) n°863/2007 du 2007/2004 du Conseil et la décision 2005/267/CE du Conseil - Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et bureaux de l'Union et sur la libre circulation de ces données

	- Règlement (UE) 2019/1896 du parlement européen et du conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes et abrogeant les règlements (UE) n°1052/2013 et (UE) 2016/1624
Comment obtenir communication et rectification des données ?	Dans le cadre du traitement de données relatif au système de surveillance des retours forcés (SGRF) Le droit d'accès, le droit de rectification, le droit à l'effacement, le droit de s'opposer au traitement se fait auprès du délégué à la protection de Frontex à dataprotectionoffice@frontex.europa.eu
Remarques	« *Une enquête de trois médias européens, dont Le Monde, révèle que l'agence européenne de surveillance des frontières a collecté les données de centaines de milliers de personnes, migrantes et militantes, et les a transférées à Europol, l'agence de coopération policière entre États membres. Des pratiques illégales, épinglées dans un rapport du Contrôleur européen de la protection des données.* » (InfoMigrants, « Frontex a délivré illégalement les données de 13 000 migrants et militants aux polices européennes, selon une enquête », 2025) Comme le rappelle StateWatch : « *Le projet « Personal Data for Risk Analysis » (PeDRA), lancé conjointement avec Europol, a cherché à utiliser les données collectées par Frontex à partir d'entretiens de « débriefing » avec des migrants pour alimenter les bases de données et les analyses d'Europol. Face à l'opposition de ses propres responsables de la protection des données, Frontex a cherché à recueillir des données génétiques et des données sur l'orientation sexuelle, et à recueillir des informations non seulement auprès de personnes soupçonnées d'être impliquées dans des activités criminelles, mais aussi auprès de victimes et de témoins.* » (StateWatch, « Frontex and interoperable databases : knoweldge as power ? », 2023)
Sources	Euractiv, « Frontex : le Contrôleur européen de la protection des données tire la sonnette d'alarme sur le traitement des données des migrants », 2023 Frontex, « Artificial Intelligence - based capabilities for European Border and Coast Guard », 2021 Frontex, « Weak Signals in Border Management and Surveillance Technologies », 2022 Gisti, « Frontex, l'agence européenne d'expulsion », in Plein droit, 2020 InfoMigrants, « Frontex a délivré illégalement les données de 13 000 migrants et militants aux polices européennes, selon une enquête », 2025 Le Monde, « Migrants : comment Frontex a alimenté de manière illicite les polices européennes avec les données personnelles de milliers de personnes », juillet 2025 Migreurop, Frontex, une agence européenne hors de contrôle, Note, 2021 StateWatch, « Frontex and interoperable databases : knoweldge as power ? », 2023

Nom	**INTERPOL**
Sens de l'acronyme	International Criminal Police Organization / Organisation internationale de police criminelle
Date de création	7 septembre 1923
Quelle échelle ?	Internationale
Objectifs officiels	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 196 États membres d'Interpol 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 ». Les fichiers d'Interpol reposent sur deux grands axes de principes : - *« Les principes relatifs à la coopération policière internationale »* - *« Les principes relatifs au traitement de l'information »* Les objectifs d'Interpol sont : - « *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 ;* - *Établir et développer toutes les institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun (Article 2 du Statut d'Interpol) 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 : - 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 événement, 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 ; - Mener des activités de gestion des frontières et des contrôles aux frontières ; - Identifier des menaces, des tendances en matière de criminalité ainsi que des réseaux criminels. (Article 10 du règlement d'Interpol sur le traitement des données)
Objectif implicite	Interpol participe à la criminalisation des personnes en migration en associant les fichiers de contrôle des migrations et des fichiers de sécurité. En 2013 l'ONG Fair trials relève que l'usage d'Interpol peut être instrumentalisé à des fins politiques et porter préjudice voire mettre en danger les personnes fichées, notamment les personnes quittant leur pays. (Fair Trails International, « Strenghtening respect for human rights, strenghtening Interpol », 2013)
Contenu des données	Plusieurs fichiers et bases de données : - Bibliothèque numérique INTERPOL d'alerte sur les documents de voyage (DIAL-DOC) - Base de données génétiques* - Système électronique de documentation et d'information sur les réseaux d'enquêtes avec informations sur les documents de voyage (EDISON) - Base de données sur les empreintes digitale (AFIS) - Bases de données internationales sur l'exploitation sexuelle des enfants (ICSE) - Réseau d'information balistique d'INTERPOL (IBIN) - Système d'information* criminelle d'INTERPOL (ICIS) – base de données nominatives - Système de reconnaissance faciale d'INTERPOL (IFRS) - Tableau de référence INTERPOL des armes à feu (IFRT) - Système INTERPOL de gestion des données sur les armes illicites et du traçage des armes (iARMS) - RELIEF base de données spécialisée dans l'analyse du trafic de stupéfiants - Base de données sur les documents administratifs volés (SAD) - Base de données SLTD (documents d'identité et de voyage) - Base de données sur les véhicules automobiles volés (SMV) - Base de données sur les bateaux volés (SVD) - Base de données sur les œuvres d'art volées (WOA) - Fichiers d'analyse - Base de gestion de la conformité Liste complète des fichiers sur le site d'INTERPOL Base de données « nominatives » : Cette base contient des informations relatives aux « malfaiteurs internationaux » (selon la terminologie d'Interpol) 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 bureau central national (BCN) à 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 les titres de documents de voyage, passeports et autres documents permettant de voyager. (Voir fiche SLTD) L'accès à cette base a été étendu aux services chargés du contrôle des mouvements migratoires (consulats, points de contrôles frontaliers, aéroports internationaux...). Elle permet aux Bureaux centraux nationaux INTERPOL et à d'autres services autorisés comme les services d'immigration et la police des frontières de vérifier la validité d'un document de voyage suspect en quelques secondes. Base SMV (pour « stolen motor vehicles ») sur les véhicules volés : rassemble les identifiants de près de 5 millions de véhicules de tout type. Base données FIELDS : FIELDS est une initiative conjointe d'INTERPOL et de FRONTEX. Elle associe une version plus moderne de l'ancienne plateforme Dial-Doc d'INTERPOL avec les fiches de vérification rapide de FRONTEX, pour les mettre à la disposition des agents de première ligne chargés des contrôles aux frontières via le système mondial de communication policière sécurisée I-24/7 d'INTERPOL. (Voir fiche FIELDS) 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 de 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. Les utilisateurs autorisés des pays membres peuvent consulter, ajouter et rechercher des entrées dans la base de données d'empreintes digitales grâce au système automatisé de reconnaissance d'empreintes digitales.
Autorité(s) compétente(s)	Les Bureaux centraux nationaux et le Secrétariat général : - **Les Bureaux centraux nationaux** : chaque État 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 (ministère de l'intérieur). La gestion quotidienne du BCN est confiée à la division des relations internationales (ministère des armées). - **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*. »
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 **Les entités nationales :** les Bureaux centraux nationaux soumettent les autorisations d'accès à certains fichiers aux entités nationales compétentes. Modalités de délivrance des autorisations à l'article 21 du règlement d'Interpol sur le traitement des données **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
Durée de conservation des données	**Voir la liste des durées de conservation des données qui varient entre 5 ans à 30 ans.**
Échanges de données avec d'autres fichiers ?	Les informations concernant les interconnexions sont difficiles à trouver. Néanmoins, l'article 55 du règlement d'Interpol sur le traitement des données, mentionne les conditions nécessaires pour l'interconnexion d'Interpol avec d'autres fichiers : « *Toute opération d'interconnexion doit répondre aux conditions cumulatives suivantes :* - *La finalité, la nature et l'étendue de l'interconnexion sont déterminées, explicites et conformes aux buts et activités de l'Organisation ;* - *L'interconnexion présente un intérêt pour la coopération policière internationale ; le système d'information* à interconnecter offre un niveau de sécurité au moins équivalent à celui du Système d'information* d'INTERPOL ;* - *L'interconnexion permet le respect des conditions de traitement fixées par les sources des données contenues dans le Système d'information* d'INTERPOL et dans le système d'information* à interconnecter ;*

	- *L'interconnexion permet la notification immédiate, au Bureau central national, à l'entité nationale ou à l'entité internationale qui a introduit des données dans le Système d'information* d'INTERPOL ainsi qu'au Secrétariat général, de tout élément issu des données interconnectées susceptible de présenter un intérêt pour la coopération policière au niveau international.* » D'après les données que nous avons recoupé, il y'a des interconnexions avec les fichiers FAED, FNAEG, FOVeS, FPR, TAJ, TES, CIR, ETIAS, SIS II, VIS, API-PNR.
Textes 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 Règlement disponible sur le site d'Interpol, rubrique « Documents juridiques » - Statut d'Interpol I/CONS/GA/1956 du 13 juin 1956, disponible sur le site d'Interpol, rubrique « 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. La commission analyse et traite uniquement les requêtes formulées par écrit et étayées par des documents écrits, et elle a – sauf à titre d'exceptions – recours à des auditions. La requête suivante (voir Comment saisir la Commission – Interpol), doit être envoyé à CCF@interpol.int 2. Ces droits d'accès, 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) En France, il est possible de s'adresser à la Commission de contrôle des fichiers d'Interpol (200 quai Charles de Gaulle, 69006 Lyon) pour demander l'accès, la rectification et l'effacement des données. (Article 18 du règlement sur le traitement des données d'Interpol, et règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol) **Il existe un guide de procédure à l'attention des demandeurs qui saisissent la Commission.** (CCF Procedural guidelines for applicants FR)
Remarques	Comme le relève Hélène Legeay, 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 États peuvent mettre leur véto à la transmission d'information des personnes fichées par Interpol sur la liste rouge. (Hélène Legeay/ACAT, « Interpol, au-dessus des lois ? », 2014)
Sources	Site d'Interpol, voir les différentes rubriques citées ci-dessus JurisClasseur Droit international, Fasc. 409-10 : « ENTRAIDE JUDICIAIRE INTERNATIONALE. – Organisation internationale de police criminelle – Interpol », 15 juin 2018 Hélène Legeay/ ACAT, « Interpol, au-dessus des lois ? », 4 septembre 2014 Fair Trials International, « Strenghtening respect for human rights, strenghtening Interpol », novembre 2013

Glossaire[38]	
Accès direct	Les fichiers institués directement autour des personnes étrangères soit dans un but de gestion soit en tant que fichiers de police
Accès indirect	Les fichiers où l'enregistrement de données relatives à la condition de personnes étrangères (dites données sensibles) dans des fichiers nationaux et pouvant avoir des conséquences du fait de ce statut (par exemple non-obtention du titre de séjour ou de son renouvellement).
Application	« Une application est un type spécifique de logiciel conçu pour accomplir une tâche particulière pour l'utilisateur. Les applications peuvent être installées sur un ordinateur, une tablette ou un téléphone. Contrairement aux logiciels systèmes, les applications sont utilisées pour des tâches spécifiques ». (Comparateur CPGI)
Carnet et fiche anthropométrique	Le carnet anthropométrique a été créé en France en 1912 pour contrôler la circulation des « nomades » sur le territoire, où était décrit des traits physiques des personnes pour les identifier. La fiche anthropométrique présente l'ensemble des antécédents judiciaires d'une personne. Elle est toujours utilisée actuellement par les administrations.
Consultation des données	La consultation permet d'accéder à des données personnelles, d'obtenir une copie, de connaître les finalités du traitement et les catégories de données. Elle peut renvoyer au droit d'accès ou à une autorisation et/ou habilitation spécifique.
Base de données	Les bases de données sont des « systèmes d'information permettant le traitement d'un même ensemble de données personnelles, avec tous les composants, réseaux et applications impliqués dans ces traitements et l'accès aux données (que celles-ci soient ou non contenues dans une ou plusieurs « bases de données » au sens technique). » (Cnil)
Destinataires des données / ont accès aux données	Les destinataires sont des personnes habilitées à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions. (Règlement général sur la protection des données) Les personnes qui ont accès aux données peuvent consulter les données personnelles, obtenir une copie, connaître la finalité du traitement et les catégories de données ainsi qu'inscrire les personnes dans le fichier lorsqu'elles possèdent une habilitation.
Directive « Police-Justice »	Directive (UE) n° 2016/680 du 27 avril 2016. La directive « Police-Justice » établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données personnelles par les autorités compétentes pour les enquêtes et les poursuites pénales. (Cnil)
Données alphanumériques	« Dans un fichier informatique les données sont alphanumériques, c'est à dire numériques ou alphabétiques ou encore mixtes. L'ordinateur traite généralement les données comme étant alphanumériques : les caractères, lettres ou chiffres sont codés de 0 à 255 (code ASCII = American Standard Code for Information Interchange). » (Université Claude Bernard Lyon 1)
Données biométriques	« Les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques » (Règlement général sur la protection des données)
Données dactyloscopiques	« Les images d'empreintes digitales et les images d'empreintes digitales latentes qui, en raison de leur caractère unique et des points de référence qu'elles contiennent, permettent de réaliser des comparaisons précises et concluantes en ce qui concerne l'identité d'une personne » (Règlement (UE) 2019/817)
Données génétiques	« Les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » (Règlement général sur la protection des données)
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.

[38] Dans le cadre de cet outil, l'Anafé ne définit pas les termes de « sûreté publique, sûreté de l'État, atteinte à un intérêt fondamental de la nation, d'ordre public », etc.

	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 lorsqu'il a été expressément écarté par l'acte autorisant le traitement.
Fichier	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) « 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. » (Cnil) Le terme de « fichier » est souvent utilisé de manière alternative avec les termes « traitement de données* personnelles » ou « système d'information* ».
Inscription automatique	L'Anafé n'a pas trouvé de définition légale de cette notion mais l'interprète comme suit : lors de la création d'une fiche sur un fichier, les éléments récoltés seront inscrits automatiquement dans le ou les autres fichiers avec lesquels il est interconnecté.
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. » (Conseil d'État, 19 juillet 2010, n° 317182) La Cnil identifie 3 critères cumulatifs définissant l'interconnexion : • L'objectif est « la mise en relation de fichiers ou de traitements de données à caractère personnel » ; • « Cette mise en relation concerne au moins deux fichiers ou traitements distincts » ; • « Il s'agit d'un processus automatisé ayant pour objet de mettre en relation des informations issues de ces fichiers ou de ces traitements ».
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 : 1. Une interface de recherche unique permettant d'interroger simultanément plusieurs systèmes d'information et de produire des résultats combinés sur un seul écran. 2. L'interconnexion des systèmes d'information, qui permet aux données enregistrées dans un système d'être automatiquement consultées par un autre système. 3. La mise en place d'un service partagé de mise en correspondance de données biométriques* à l'appui de divers systèmes d'information. 4. Un répertoire commun de données pour différents systèmes d'information (module central). (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.)
Journalisation	Les outils de journalisation permettent d'enregistrer, de stocker et d'analyser des événements et des données système. Comme le rappelle la Cnil : « Le but des outils de journalisation est, particulièrement dans le contexte de systèmes multi-utilisateurs, d'assurer une traçabilité des accès et des actions des différentes personnes accédant aux systèmes d'informations et, plus précisément, aux traitements de données personnelles mis en œuvre au sein de leurs organisations. » (Cnil, recommandation relative aux mesures de journalisation, 2021)
Logiciel	« Un logiciel est un ensemble de programmes et de données qui permettent à un ordinateur de fonctionner. Il s'agit d'un terme général qui englobe divers types de programmes informatiques. Les logiciels incluent les systèmes d'exploitation, les utilitaires système et de nombreux autres programmes qui permettent à un ordinateur de répondre à différents besoins. » (Comparateur CPGI)

Loi Informatique et Libertés	Loi n° 78-17 du 6 janvier 1978 : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » (Article 1 modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, pour se conformer au règlement général de protection des données)
Mise en relation	L'Anafé n'a pas trouvé de définition légale de cette notion mais l'interprète comme suit : il s'agit d'un rapprochement informel entre au moins deux fichiers.
Papillaire	« Les traces papillaires regroupent l'ensemble des traces laissées (souvent de manière involontaire) sur un support par l'apposition d'une zone de la peau présentant des crêtes papillaires. Il s'agit de la face interne des mains (zones digitales et palmaires) mais aussi des pieds (zones plantaires). Le dessin papillaire présent sur ces différentes zones étant permanent et unique, il est donc possible, à partir d'une trace papillaire, d'identifier son auteur. » (PJGN)
Règlement général de protection des données	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Le RGPD « établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. [Le RGPD] protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. » (Cnil)
Rapprochement de données	« Le rapprochement, tout comme l'interconnexion, constitue une mise en relation d'informations. Cependant, le rapprochement se distingue de l'interconnexion sur deux points : • À la différence d'une interconnexion, un rapprochement ne suppose pas nécessairement la mise en œuvre de moyens automatisés. Ainsi, la comparaison visuelle d'informations issues de deux fichiers ou encore l'enrichissement d'un fichier existant par saisie manuelle d'informations issues d'un autre fichier ne constituent pas une interconnexion, mais de simples rapprochements. • Un rapprochement peut être réalisé au sein d'un même traitement ou fichier, alors qu'une interconnexion implique deux fichiers distincts. » (Cnil)
Routeur	« Un routeur est un équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau. Il permet, entre autres, de faire circuler des données entre deux interfaces réseau. Il peut également être présenté comme une passerelle entre plusieurs serveurs et facilite alors l'accès aux ressources disponibles sur le réseau pour les utilisateurs. » (Le Journal du Net)
Serveur informatique	« Le terme serveur désigne le rôle joué par un appareil matériel destiné à offrir des services à des clients en réseau Internet ou intranet. La taille du support physique d'un serveur varie d'un simple boîtier à une ferme de calcul, selon le nombre d'utilisateurs susceptibles de le solliciter simultanément. » (Le Journal du Net)
Système d'information	« Ensemble de composants interconnectés visant à collecter, stocker, traiter et diffuser l'information dans une organisation. Ses objectifs vont de la facilitation de la prise de décision à l'optimisation des processus internes, en passant par l'amélioration de la communication et de la collaboration » (DataScientest)
Traitement de données	« Une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement). [...] Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. » (Cnil)
Transfert de données	Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne (Règlement général sur la protection des données)

Abréviations	
ADN	Acide DésoxyriboNucléique
ANTS	Agence nationale des titres sécurisés
ARS	Agence Régionale de Santé
ASE	Aide sociale à l'enfance
BCE	Banque centrale européenne
BCN	Les Bureaux centraux nationaux (d'Interpol)
BMS	Système de Gestion de Batterie
CASF	Code de l'action sociale et des familles
CE	Conseil d'État
CEDH	Cour européenne des droits de l'Homme
CESEDA	Code de l'entrée et du séjour des étrangers et du droit d'asile
CEPOL	Agence de l'Union européenne pour la formation des services répressifs
CIPDR	Comité interministériel de prévention de la délinquance et de la radicalisation
CNAPR	Centre national d'assistance et de prévention de la radicalisation
CNDA	Cour nationale du droit d'asile
CNCDH	Commission nationale consultative des droits de l'Homme
CNI	Carte nationale d'identité
Cnil	Commission nationale de l'informatique et des libertés
COSSEN	Commandement spécialisé pour la sécurité nucléaire
DCPJ	Direction nationale de la police judiciaire
DDHC	Déclaration des droits de l'Homme et du citoyen
DGEF	Direction générale des étrangers en France
DGGN	Direction générale de la gendarmerie nationale
DGPN	Direction générale de la police nationale
DGSI	Direction générale de la sécurité intérieure
DINUM	Incubateur interministériel des services numériques
DNPAF	Direction nationale de la police aux frontières
DRI	Direction des relations internationales
DRPP	Direction du renseignement de la préfecture de Police
EMCDDA	Observatoire européen des drogues et des toxicomanies
ESP	Portail de recherche européen
EUROJUST	Agence de l'Union européenne pour la coopération judiciaire en matière pénale
FNAD	Fichier des non admis
FRONTEX	Agence européenne de garde-frontières et garde-côtes
GED	Gestion électronique des documents
GISTI	Groupe d'information et de soutien des immigré.e.s
HCR	Haut-commissariat des Nations unies pour les réfugiés
IDPP	Institut de prévention et de protection
IRIS	Ilots regroupés pour information statistique
ITF	Interdiction du territoire français
LDH	Ligue des droits de l'Homme
MID	Détecteur d'identités multiples
OFII	Office français de l'immigration et de l'intégration
OFPRA	Office français de protection des réfugiés et apatrides
OIM	Organisation internationale pour les migrations
OLAF	Office européen de lutte antifraude
OLE	Officier de liaison européen
OQTF	Obligation de quitter le territoire français
PAF	Police aux frontières
PJGN	Police judiciaire de la gendarmerie nationale
RGPD	Règlement général sur la protection des données
SIAO	Service intégré d'accueil et d'orientation

SIRENE	Système informatique pour le répertoire des entreprises et des établissements.
SCRT	Service central du renseignement territorial
SGRF	Système de surveillance des retours forcés
SNEAS	Service national des enquêtes administratives de sécurité
UCLAT	Unité de coordination de lutte anti-terroriste
UE	Union européenne
UIP	Unité d'information des passagers