# L'identification numérique des ressortissants d'États tiers : de la multiplication des bases de données à leur interopérabilité (1)

**Émilie Destombes**, Doctorante contractuelle à l'université de Bordeaux - Centre de recherche et de documentation européennes et internationales (CRDEI) - Centre de documentation et de recherches européennes (CDRE)

**Résumé**

Cette contribution vise à souligner que l'identification est devenue une finalité propre légitimant la multiplication des bases de données et leur interopérabilité. Il s'agit donc d'analyser l'évolution de l'identification pour pouvoir mesurer son impact sur le respect des droits fondamentaux des ressortissants d'États tiers.

**Summary**

This contribution aims to stress that identification has become a specific purpose legitimizing the multiplication of databases and their interoperability. The purpose is therefore to analyse the evolution of identification in order to be able to measure its impact on the respect for the fundamental rights of third-country nationals.

***Etude***

Les règlements du 20 mai 2019 relatifs à l'interopérabilité des systèmes d'information de l'Union européenne (UE), en impactant les procédures d'identification, caractérisent à la fois un mouvement de continuité mais aussi de rupture au sein des politiques européennes.

L'interopérabilité aspire à rendre les « systèmes d'information plus robustes et plus intelligents au service de la frontière et de la sécurité » (2). Les bases de données constituent ainsi un outil de démarcation des frontières extérieures de l'UE. Ces éléments immatériels apportent la preuve que la notion de frontière ne peut plus se définir seulement comme une ligne séparant les territoires respectifs de deux États (3) mais aussi comme un régime de régulation de la circulation des personnes qui se caractérise au sein de l'UE par la création de l'espace de liberté, de sécurité et de justice (ELSJ). Ce régime conduit à repousser la vigilance des autorités sur les frontières extérieures : l'ELSJ repose, depuis ses origines, sur une « démarche sécuritaire quasi exclusive » (4). L'abolition des frontières intérieures est devenue un motif pour adopter des instruments de contrôle étatique. La transmission d'informations entre les autorités administratives des États membres apparaît alors comme une « mesure compensatoire » au déficit sécuritaire (5) et se concrétisera dès 1990 avec la Convention d'application de l'accord de Schengen qui permettra l'adoption de la première base de données : le système d'information Schengen (SIS). Le caractère essentiel de la transmission d'information a ainsi conduit à la généralisation des fichiers et des bases de données à l'égard principalement des ressortissants d'États tiers dans le but de leur identification. Or cette généralisation n'est pas seulement quantitative, elle devient de plus en plus intrusive (6). Cette banalisation se retrouve dans le concept de

frontière intelligente, qui démontre une « radicalisation des procédures de contrôle » (7), renouvelant « l'art des limites » (8) du régime frontalier européen. Ainsi, cette réforme marque la continuité de la logique sécuritaire par le développement d'un espace de contrôle.

Pour autant, une telle logique apparaît résolument en rupture par rapport à l'idéologie libérale consistant, au nom des libertés individuelles, à la limitation du pouvoir politique. Cette rupture s'explique par un brouillage terminologique entre les notions de sûreté et de sécurité conduisant à l'adoption de mesures reposant sur « l'illusion d'une vie sans dangers et légitim[ant] l'intrusion dans les libertés individuelles » (9).

La récupération politique du postulat de déficit sécuritaire est topique s'agissant du droit des étrangers. Il mène au développement technologique du régime frontalier qui par le jeu du fonctionnalisme conduit à l'appréhension de termes techniques qui visent à permettre un consensus en dépolitisant les enjeux relatifs à la datasurveillance. L'identification apparaît comme une nécessité et suscite la recherche d'une complétude d'information : elle est une source objective à la généralisation des bases de données (I). Or la recherche d'une identification précise conduit *in fine* à l'octroi de renseignements et se transforme alors en un fondement subjectif à la généralisation des bases de données (II).

## I. - L'identification, fondement objectif à la généralisation des bases de données

Le déficit d'information, inhérent à l'altérité du ressortissant d'un État tiers, a été analysé comme un déficit de sécurité contribuant à rendre l'ELSJ vulnérable. Divers instruments ont été adoptés de façon à identifier efficacement, *in concreto*, les ressortissants d'États tiers pour permettre aux autorités étatiques d'exercer souverainement l'activité de régulation de circulation des personnes (A). Dans un approfondissement *in abstracto* de la logique liant le déficit d'information au déficit d'identification précise est apparue la nécessité d'une efficience de l'utilisation des données (B). Or le développement de la procédure européenne d'identification joue un rôle crucial en influençant le concept d'illégalité (10) au regard de la catégorisation qu'il opère (11).

### A - L'identification, source classique d'accès aux données *in concreto*

L'apparition d'une police de l'identité (12) au niveau étatique est ancienne. Son institutionnalisation remonte aux XVI$^{e}$ et XVII$^{e}$ siècles et conduit très vite à une standardisation internationale des documents d'identité au regard des circulations internationales (13). Alors que « l'identité civile » est codifiée à l'échelle internationale, « l'identité sociale » est encadrée au niveau étatique. Il y a donc une identification différenciée *in concreto* selon la politique menée. L'accès à l'information est limité et ce même au niveau national afin de garantir le respect de la vie privée (14). Les éléments d'identification, c'est-à-dire les données à caractère personnel, sont donc accessibles à condition que cela soit nécessaire. Tel est bien le mouvement opéré par la création de bases de données distinctes (15). La légitimité de la collecte des données à caractère personnel est ainsi fondée sur le principe de finalité. Le caractère cardinal de ce principe se trouve renforcé au regard du propriétaire des critères d'identification. Par les bases de données, les autorités administratives détiennent désormais des informations à caractère personnel, ce qui constitue une différence majeure avec les documents présentés lors de contrôle confirmant l'identité de la personne. La multiplication des bases de données (16) mais aussi de leurs propres finalités (17) conduit à un accès élargi aux éléments d'identification (18). Elle interroge en ce que ce n'est plus une politique publique, ayant une finalité propre, qui conduit à l'élaboration de nouveaux systèmes d'identification. Par la perméabilité des notions d'illégalité et de criminalité induite (19), c'est l'existence des systèmes actuels qui devient une justification pour la création d'autres systèmes. L'accès à l'information est devenu une quête permettant de préserver l'ordre public - notion fuyante par essence (20) - et entraîne une collecte massive de données

personnelles (21). L'efficacité de préservation de l'ordre public conduit, par ailleurs, à recourir à des éléments d'identification de plus en plus sensibles. Les données biométriques, du fait de leur caractère précis, apparaissent plus fiables que les données alphanumériques. L'identification devient une étape qui soumet davantage le ressortissant d'un État tiers à une prise en charge par les institutions dont il est mis à l'écart (22). Or cette exclusion conduit à amoindrir *de facto* le droit à un recours effectif par la preuve diabolique qu'elle impose face à des sources d'identification encore imparfaites (23). La convergence des éléments d'identification et l'extension des finalités des bases de données par le biais des différentes révisions, présentes ou à venir, sont présentées comme un élément de préconfiguration de leur interopérabilité (24) en instaurant une convergence des procédures d'identification indépendamment du contexte de la collecte des données.

### B - L'identification, source renouvelée d'utilisation des données *in abstracto*

L'interopérabilité vise à aider la prise de décision en fournissant une image plus complète de la personne (25). Par son approche globale de l'accès aux données (26), elle constitue une étape décisive dans le droit à la protection des données personnelles : l'objectif d'ordre public, au sens large, conduit à faire abstraction des circonstances de la cause de la collecte des données. Alors que le principe de finalité avait déjà été entamé par l'extension des finalités des bases de données existantes, l'interopérabilité accentue cette tendance (27). Ainsi, « l'argument avancé maintenant est précisément le contraire - plutôt que de reconnaître la valeur de systèmes distincts et clairement définis, l'accent est passé à une utilisation plus généralisée des données disponibles, axée sur la fixation d'une identité numérique unique aux individus » (28). La réforme est critiquée au regard des outils instaurés qui conduisent à nouveau à la création de bases de données pour parvenir à rendre les différentes bases de données interopérables. Tel est notamment le cas du répertoire commun d'identité (CIR). Le CIR est créé de façon à collecter les données biométriques et biographiques des ressortissants d'États tiers dans un dossier individuel unique regroupant les données contenues dans différentes bases de données : le système d'entrée/sortie (EES), le système d'échange d'information sur les casiers judiciaires (ECRIS-TC), le système européen d'information et d'autorisation concernant les voyages (ETIAS), le système d'information concernant les empreintes digitales en matière d'asile (Eurodac) ainsi que le système d'information sur les visas (VIS). Comparé à l'image d'un panoptique européen (29), il contribue à permettre une identification plus précise face aux données répertoriées dans les différents systèmes d'information qui peuvent « concerner la même personne, mais sous des identités différentes ou incomplètes » (30). L'efficacité de l'identification contribue à détourner « l'approche compartimentée entre les bases de données par l'interopérabilité » (31). Le recoupement des données (32) conduit le Contrôleur européen de la protection des données (CEPD) à constater les « conséquences juridiques et sociétales profondes » (33) en instituant une généralisation de masse potentiellement en violation des droits européens (34). Ainsi, le CEPD souligne les possibles divergences entre le raisonnement juridique et l'expertise scientifique. Comme le souligne Édouard Dubout, « le discours scientifique pénètre également celui du droit » (35). Ici, l'expertise numérique emprunte bien la logique du test d'aptitude : il s'agit de savoir quelle technique numérique est la plus cohérente pour parvenir à identifier les ressortissants d'États tiers dans un but de préservation de l'ordre public. Le droit se distingue de cette logique par le contrôle de proportionnalité, conduisant à justifier notamment la nécessité et la proportionnalité de la mesure (36). Or ces derniers critères sont impactés par l'érosion de la limitation des finalités des bases de données qui conduit à l'octroi d'informations subjectives, celles-ci ayant fait l'objet d'une perception particulière par les autorités étatiques.

## II. - L'identification, fondement subjectif à la généralisation des données

Les bases de données, visant l'identification des ressortissants d'États tiers, n'apportent pas seulement des informations. Elles sont également productrices de renseignements (37) lorsqu'elles permettent le contrôle

de l'identification du ressortissant d'un État tiers (A). L'effet de ces renseignements est problématique en ce qu'il entraîne une logique de préemption des données en matière d'identification (B).

**A - Le renseignement dans le contrôle de l'identification**

Les règlements en matière d'interopérabilité ne font pas référence aux renseignements qu'ils produisent. Pour autant, les outils instaurés constituent un traitement des données. Le plus explicite concerne le détecteur d'identité multiple (MID) qui consiste à lier les données des systèmes d'information de l'UE, figurant dans le CIR et le SIS, pour permettre la détection d'identités multiples. Ce premier service de renseignement pose la question de la qualité suffisante des données (38). Ainsi, s'« il est important de comprendre que l'interopérabilité ne conduit pas en soi à une amélioration de l'exhaustivité, de l'exactitude et de la fiabilité des données » (39), elle constitue en revanche le fondement juridique pour conduire à l'harmonisation des exigences en matière de qualité des données et donc à terme à l'harmonisation des procédures d'identification, sans même mesurer l'ampleur de la fraude d'identité (40). Or, si les valeurs inscrites au sein de l'article 2 du Traité sur l'Union européenne (TUE) avaient constitué le « moteur de l'action de l'Union », l'étude d'impact aurait conduit à vérifier la nécessité de la mesure en prenant en compte la fréquence de l'identification ainsi que l'évaluation des procédures d'identification afin de mesurer en quoi les capacités sont insuffisantes. Bien qu'inscrit à de nombreuses reprises au sein des règlements, le respect des droits fondamentaux apparaît secondaire par rapport à l'impératif de sécurité et interroge au regard des effets de l'interopérabilité. En effet, la création du CIR implique l'accès à des renseignements : par la création d'un dossier individuel, il permet de connaître la concordance d'une information en cas de présence des données présentées au sein d'un des sous-systèmes. En ce sens, le CEPD a souligné que le simple fait de connaître la présence de données est un renseignement qui peut influencer la prise de décision (41) et ce alors que l'encadrement large du CIR risque de conduire à l'utilisation routinière (42). Les renseignements produits par les bases de données, qu'ils soient explicites ou implicites, ont des conséquences importantes sur le contrôle de l'identification et ce d'autant plus quand il s'agit d'une identification anticipée.

**B - Le renseignement dans la projection de l'identification**

En décrivant l'évolution des bases de données, Niovi Vavoula note trois temps : celui de la modernisation du contrôle par la création des bases de données, suivi par le développement de ces dernières face au terrorisme et enfin de la généralisation de la surveillance de mouvements des ressortissants d'États tiers. Elle note, à partir du 11 septembre 2001, une transformation des bases de données au regard de l'impératif sécuritaire qui s'accentue au fur et à mesure des réformes en réponse aux différentes attaques terroristes. Ainsi, elle met en avant la double fonctionnalité de la biométrie au sein de ces bases de données : s'il est possible d'utiliser les données biométriques dans le but d'une vérification d'identité, de telles données peuvent aussi être utilisées en tant qu'outil d'investigation. Les capacités d'investigations ont été renforcées plus récemment visant désormais l'anticipation des infractions, des délits ou des crimes potentiels. L'introduction de la notion de « risque » au sein des bases de données traduit ainsi le diagnostic par les autorités de la dangerosité et non plus de la culpabilité de la personne et manifeste « l'émergence, voire l'installation d'un droit pénal de l'ennemi » (43). Outre les risques de discrimination qu'il risque d'instaurer (44), il conduit paradoxalement à une dépersonnalisation du droit migratoire (45).

Aujourd'hui limitée aux ressortissants d'États tiers mais transposable dès demain à l'ensemble des migrants au sein de l'UE, l'identification numérique impacte l'effectivité non seulement du droit à la protection des données à caractère personnel mais aussi plus largement la logique spécifique des droits fondamentaux.

(1) L'auteur remercie la relecture attentive de M. D. Szymczak, professeur à Science Po Bordeaux.
(2) Commission européenne, COM(2016) 205 final, 6 avr. 2016.
(3) L. Imbert, L'agence Frontex au prisme du concept polysémique de frontière, *in* C. Chevallier-Govers et R. Tinière (dir.), De Frontex à Frontex. Vers l'émergence d'un service européen de garde-côtes et garde-frontières, Bruxelles, 2019. 150.
(4) H. Labayle, Schengen, un coupable idéal, GDR, 25 nov. 2015, www.gdr-elsj.eu/2015/11/25/frontieres/schengen-un-coupable-ideal.
(5) E. Brouwer, *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden, Martius Nijhoff Publishers, 2008. 13.
(6) M. Delmas-Marty, Libertés et sûreté dans un monde dangereux, Seuil, 2010. 68.
(7) *Ibid*.
(8) M. Foucher, L'obsession des frontières, Paris, Perrin, 2012. 7.
(9) M. Delmas-Marty, *op. cit.*, p. 23.
(10) B. Menezas Quieroz, *Illegality staying in the EU - An analysis of illegality in EU Migration Law*, Londres, Hart Publishing, 2018. 117.
(11) S. Barbou des Places, La catégorie en droit des étrangers : une technique au service d'une politique de contrôle des étrangers, Revue Asylon(s), n° 4, mai 2008.
(12) P. Mbongo, Identité (police de l'), *in* F. Hervouët, P. Mbongo et C. Santulli (dir.), Dictionnaire encyclopédique de l'État, Berger-Levrault, 2014. 530.
(13) *Ibid.*, p. 530-536.
(14) CEDH, 2 févr. 2010, n° 21924/05, *Sinan Isik c/ Turquie*, AJDA 2010. 997, chron. J.-F. Flauss ; D. 2011. 193, obs. J.-F. Renucci ; RFDA 2011. 987, chron. H. Labayle et F. Sudre.
(15) E. Brouwer, *op. cit.*, p. 142-143.
(16) V. en ce sens la contribution dans ce dossier de C. Dire, Le concept de « gestion intégrée des frontières ».
(17) V. en ce sens la contribution dans ce dossier d'E. Cornuz Rigaud, Les implications de l'interopérabilité au regard des droits fondamentaux.
(18) E. Brouwer, *Interoperability and Interstate Trust : a Perilous Combination for Fundamental Rights*, 11 juin 2019, http://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights.
(19) B. Menezas Quieroz, *op. cit.*, p. 117.
(20) A. Ianniello-Saliceti, La protection des données personnelles et l'introuvable définition de l'ordre public, *in* C. Chevallier-Govers et R. Tinière (dir.), *op. cit.*, p. 503.
(21) J. Jeandesboz, *Smartening border security in the European Union : An associational inquiry, Security Dialogue*, vol. 47, n° 4, 2016. 292.
(22) L. Azoulai, Le droit européen de l'Immigration, une analyse existentielle, RTD eur. 2018. 519.
(23) FRA, *Fundamental rights and the interoperability of EU information systems : borders and security*, 7 juill. 2017. 31-32.
(24) G. Mirja *et al., Interoperability of Justice and Home Affairs Information Systems. Civil liberties, justice and home affairs*, PE604.947, avr. 2018. 29-30.
(25) FRA, préc., p. 7.
(26) N. Vavoula, *Databases for Non-EU Nationals and Right to Private Life : Towards a System of Generalised surveillance of Movement, in EU Law in Populist Times*, Cambridge University Press, 2020. 227.
(27) V. en ce sens la pluralité des finalités poursuivies par le règlement (UE) n° 2019/817, consid. 9.

(28) C. Jones, *Data Protection, Immigration Enforcement and Fundamental Rights : What the EU's Regulations on Interoperability Mean for People with irregular Status*, PICUM, 2019, https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf, p. 16.
(29) V. en ce sens la référence faite à D. Bigo par N. Vavoula, *op. cit.*
(30) Règl. UE n° 2019/817, consid. 22.
(31) G. Mirja *et al.*, préc., p. 64.
(32) J. Burchett, Frontex et l'interopérabilité des systèmes d'information. Réflexion à propos de l'articulation entre les impératifs de sécurité et de liberté, *in* C. Chevallier-Govers et R. Tinière (dir.), *op. cit.*, p. 104.
(33) CEPD, avis 4/2018, 16 avr. 2018, sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'Union européenne, p. 3.
(34) CJUE, gr. ch., 8 avr. 2014, aff. jtes C-293/12 et C-594/12, *Digital Rights Irland*, AJDA 2014. 773 ; *ibid*. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1355, et les obs., note C. Castets-Renard ; *ibid*. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; Légipresse 2014. 265 et les obs. ; RTD eur. 2014. 283, édito. J.-P. Jacqué ; *ibid*. 2015. 117, étude S. Peyrou ; *ibid*. 168, obs. F. Benoît-Rohmer ; *ibid*. 786, obs. M. Benlolo-Carabot - CEDH, 18 avr. 2013, n° 76100/13, *M. K. c/ France*.
(35) E. Dubout, La fin du droit ? Droit, politique et expertise scientifique en période de crise sanitaire, Jus Politicum, 21 avr. 2020.
(36) H. Fulrichon, Vers un rééquilibrage des pouvoirs en matière de protection des droits et des libertés fondamentales ? Libres propos du rôle du juge judiciaire en tant que juge de la subsidiarité, *in* Les droits de l'homme à la croisée des droits. Mél. F. Sudre, LexisNexis, 2018. 245.
(37) S'agissant de la distinction entre les notions d'information et de renseignement, v. T. Herran, La distinction entre l'information et le renseignement dans l'espace de liberté, de sécurité et de justice. Réflexions à propos de l'échange de données entre forces de police, *in* C. Chevallier-Govers (dir.), L'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne, Mare & Martin, 2018. 33.
(38) E. Brouwer, *Interoperability and Interstate Trust : a Perilous Combination for Fundamental Rights*, 11 juin 2019, http://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights.
(39) G. Mirja *et al.*, préc., p. 51.
(40) En ce sens J. Burchett souligne que la présentation de documents frauduleux pour l'année 2017 n'a jamais été aussi bas depuis 2013, préc., p. 105.
(41) CEPD, préc., p. 3.
(42) N. Vavoula, *op. cit.*, p. 257.
(43) T. Herran, préc., p. 35.
(44) C. Jones, préc., p. 33.
(45) B. Menezas Quieroz, *op. cit.*, p. 137.