La construction de l'État biométrique

Pouvoirs de police et discrimination

1.
Introduction 2

2.
L'identification biométrique : une priorité européenne 4

Les demandeurs d'asile : le premier groupe cible 5
Des demandeurs d'asile aux citoyens et résidents 6
Vers l'interopérabilité 6

3.
Financement des technologies biométriques 11

Biométrie et recherche sur la sécurité 12
Promouvoir les intérêts de l'État et de l'industrie 17

4.
Réseaux de technologie policière 21

5.
Technologie avancée, pratiques régressives 25

Profilage ethnique par la police 26
Interopérabilité pour les contrôles d'identité 28

6.
Conclusion 31

1.
Introduction

L'utilisation de la technologie biométrique par les États dans le but d'identifier les personnes a progressé rapidement au cours des trois dernières décennies. Initialement réservée à une utilisation dans des lieux fixes tels que les postes de police, les consulats (par exemple, pour le traitement des visas) ou les centres de détention, elle a ensuite été étendue aux frontières, les empreintes digitales et les images faciales étant désormais saisies et vérifiées aux points de passage frontaliers dans de nombreux pays du monde. Certains États ont également cherché à équiper les policiers et les fonctionnaires de l'immigration de dispositifs mobiles d'identification biométrique permettant de scanner les empreintes digitales ou les visages dans la rue pour vérifier l'identité d'une personne. Sous l'égide de l'initiative de «interopérabilité» de l'UE, qui interconnectera une multitude de bases de données personnelles différentes, ces efforts en matière d'identification biométrique mobile sont appelés à se développer considérablement.

Le présent rapport examine l'évolution des lois, projets et politiques visant à faire progresser le développement et le déploiement des technologies biométriques à des fins d'identification individuelle dans l'Union européenne au cours des deux dernières décennies. Après la mise en place de systèmes distincts pour la collecte et le stockage de données biométriques sur différentes catégories de ressortissants étrangers - demandeurs d'asile, titulaires de visas, etc. - ces données sont désormais rendues «interopérables» grâce à leur consolidation dans une base de données unique et globale. Ceci servira de base technique aux politiques visant à renforcer les contrôles d'identité, avec pour objectifs principaux la lutte contre la fraude à l'identité et l'augmentation du nombre d'expulsions.

Ceci présente des risques importants pour les droits des citoyens et des non-ressortissants. Dans un contexte de profilage ethnique bien ancré chez les forces de l'ordre, la mise à disposition de nouveaux moyens technologiques pour effectuer des contrôles d'identité risque encore d'exacerber les pratiques discriminatoires existantes. Il est donc nécessaire que les militants, activistes, avocats et chercheurs redoublent d'efforts pour enquêter, analyser et contester tant le développement et l'acquisition de nouvelles technologies de maintien de l'ordre que les lois et politiques qui sous-tendent leur utilisation.

La première section du présent rapport examine le développement progressif d'un système d'identité biométrique global au niveau de l'UE, depuis la création au début du siècle, d'Eurodac (une base de données stockant les empreintes digitales des demandeurs d'asile), jusqu'à la construction actuellement en cours du «Répertoire Commun d'Identité» (CIR *Common Identity Repository*), qui intégrera des données biométriques et alphanumériques provenant de cinq bases de données différentes à grande échelle. Il semble que les autorités nationales aient jusqu'à présent peu progressé dans l'acquisition de la technologie nécessaire pour effectuer des contrôles d'identité à l'aide du CIR, ce qui ouvre des possibilités d'interventions visant à garantir que - à tout le moins - des évaluations d'impact significatives en matière de non-discrimination et de protection des données soient réalisées avant son introduction.

La section suivante examine comment le financement public des programmes de recherche et d'innovation de l'UE a contribué au développement des technologies d'identification biométrique, en particulier celles qui ont ensuite été intégrées dans des initiatives telles que les «frontières intelligentes». Depuis 1998, l'UE a alloué quelque 290 millions € de fonds publics au développement de la technologie biométrique. Au cours des 15 dernières années, sous l'impulsion de la guerre contre le terrorisme et de la recherche de «solutions» technologiques à des problèmes tels que la criminalité, le terrorisme et l'immigration clandestine, la majeure partie de ces fonds a été consacrée à des projets de recherche axés sur les applications de la biométrie en matière de sécurité publique. Les agences de l'UE telles qu'Europol et Frontex se voient désormais attribuer un rôle dans la détermination des priorités de recherche, dans le but de garantir la prise en compte des besoins des services de police et des agences frontalières. Face à une telle évolution, un contrôle public et démocratique accru du programme est nécessaire.

Le présent rapport élucide ensuite les réseaux sous-terrains de spécialistes de la police et de la technologie qui ont cherché à affiner les politiques et les pratiques nécessaires à l'utilisation de ces technologies, avant d'examiner le contexte dans lequel ces technologies sont déployées, en l'espèce, un profilage ethnique pratiqué de longue date par les autorités chargées de l'application de la loi. L'introduction de nouvelles technologies dans ce contexte, dans le but explicite de faciliter les contrôles d'identité, risque d'entraîner un nombre croissant de contrôles injustifiés à l'encontre de citoyens et de non-citoyens issus de minorités ethniques, étant donné la manière dont la couleur de la peau est trop souvent traitée comme un indicateur du statut migratoire.

Le rapport inclut un certain nombre d'études de cas qui visent à illustrer la manière dont les États ont cherché à collecter et à utiliser les données biométriques ces dernières années, et à mettre en évidence certains des défis importants que les acteurs de la société civile ont dû relever en réponse. Il existe un nombre croissant d'initiatives qui cherchent à établir des liens entre les campagnes antiracistes, les organisations de défense des droits des migrants et les spécialistes de la technologie. Ceci va s'avérer être d'une importance vitale dans les années à venir, car les États cherchent de plus en plus à utiliser les nouvelles technologies pour faire appliquer des lois et des politiques qui divisent et excluent.

Dans un monde où les systèmes d'identification biométriques sont de plus en plus présents dans les sociétés technologiquement avancées, il n'est pas surprenant que les autorités étatiques cherchent également à utiliser ces technologies à leur profit. L'introduction de ces systèmes est généralement justifiée par le fait qu'ils permettent de réguler la mobilité internationale, de lutter contre la criminalité et le terrorisme, et de combattre l'immigration «illégale». Cela peut être en partie vrai, mais ils accordent également à l'État des pouvoirs historiquement sans précédent *vis-à-vis* de l'individu. Dans un contexte de racisme et de discrimination systémiques ainsi que face à la volonté constante des gouvernements nationaux et des institutions européennes d'identifier un nombre croissant de ressortissants étrangers afin de les expulser et/ou de les exclure de leur territoire, la tentative d'étendre et d'ancrer le déploiement et l'utilisation des technologies biométriques doit être interrogée et remise en question, dans le cadre d'une lutte plus large contre le racisme d'État et le profilage ethnique, ainsi que pour défendre l'égalité raciale et la justice sociale.

2.

L’identification biométrique : une priorité européenne

Bien que les citoyens européens soient soumis à certaines obligations en matière d'identité biométrique, jusqu'à présent les principales cibles du projet d'identité biométrique de l'UE ont été les ressortissants étrangers. À l'origine, les exigences en matière d'identité biométrique s'appliquaient aux demandeurs d'asile et aux personnes franchissant irrégulièrement les frontières de l'UE, mais les États ont étendu leur utilisation après l'avènement de la «guerre contre le terrorisme». Deux décennies plus tard, presque toutes les catégories de «ressortissants de pays tiers» qui cherchent à entrer dans l'UE ou qui y sont déjà présents doivent voir leurs données biométriques saisies et enregistrées dans l'une ou l'autre base de données à grande échelle.

Les demandeurs d'asile : le premier groupe cible

En décembre 2000, la législation établissant la base de données Eurodac a été adoptée.[1] Ce système a été créé principalement pour conserver les empreintes digitales des demandeurs d'asile, bien que, dès le départ, il ait également été utilisé pour stocker les empreintes digitales des «étrangers appréhendés à l'occasion du franchissement irrégulier d'une frontière extérieure».[2] En 2020, les autorités nationales ont transmis près de 645 000 jeux d'empreintes digitales au système central Eurodac, certains pour un stockage à long terme et d'autres pour une comparaison avec les données déjà conservées dans le système.[3]

À partir de 2015, au vu du nombre croissant de personnes arrivant dans l'UE pour demander l'asile, la Commission européenne a budgété des fonds supplémentaires pour que les États «sur la ligne de front», en particulier la Grèce et l'Italie, puissent acheter l'équipement nécessaire afin d'effectuer les inscriptions biométriques dans Eurodac.[4] Cette mesure s'inscrivait dans le cadre de «l'approche par points chauds», introduite en 2015 en tant que méthode expérimentale pour faire face à la «crise migratoire». Elle avait notamment pour objectifs d'atteindre un «taux d'empreintes digitales de 100%» pour alimenter la base de données Eurodac, qui n'était pas encore utilisée de manière systématique par l'Italie et la Grèce, dans le but de mettre un terme aux mouvements dits «secondaires» vers les États membres du Nord de l'UE. Jusqu'à présent, cette stratégie n'a pas fonctionné et les mouvements secondaires restent une priorité pour l'UE - mais le coût humain en est élevé. Dans les points chauds, les droits humains ont été subordonnés de manière intransigeante à l'enregistrement des données biométriques et aux mécanismes de contrôle.[5]

En 2016, la Commission a publié des propositions visant à étendre le système.[6] Selon ces plans, la limite d'âge pour la collecte des données serait abaissée de 14 à six ans et, à côté des empreintes digitales, Eurodac stockerait des informations biographiques et des images faciales - ces dernières afin «d'amorcer le système pour les recherches à effectuer avec un logiciel de reconnaissance faciale à l'avenir», selon la Commission européenne.[7] Des données seraient également conservées, pendant cinq ans, sur «les ressortissants de pays tiers ou les apatrides en séjour irrégulier dans un État membre». L'objectif est de transformer Eurodac en une base de données «à des fins migratoires plus larges» [8], l'un des principaux objectifs étant d'augmenter le nombre d'expulsions.[9]

1 Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32000R2725

2 Ibid.

3 Les données ne précisent pas combien de séries d'empreintes digitales sont stockées dans le système central. Voir : eu-LISA, «Consolidated Annual Activity Report 2020» https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Annual%20Activity%20Report%202020.pdf

4 Commission européenne, «EU Financial Support to Greece», 26 janvier 2017, https://ec.europa.eu/home-affairs/system/files/2017-02/20170126_factsheet_managing_refugee_crisis_eu_financial_support_greece_-_update_en.pdf, Commission européenne, «EU Financial Support to Italy», mai 2021, https://ec.europa.eu/home-affairs/system/files/2021-05/202105_managing-migration-eu-financial-support-to-italy_en.pdf

5 Voir la section «Ill-treated and arbitrarily detained for a fingerprint» dans «Hotspot Italy : How EU's flagship approach leads to violations of refugee and migrant rights» (en Anglais) , *Amnesty International*, 2016, https://www.statewatch.org/media/documents/news/2016/nov/ai-hotspot-Italy.pdf

6 Commission européenne, RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la création d'«Eurodac» pour la comparaison des empreintes digitale, COM(2016) 272 final, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52016PC0272

7 Ibid.

8 Ibid.

9 «Deportation Union», *Statewatch*, août 2020, https://www.statewatch.org/deportation-union-rights-accountability-and-the-eu-s-push-to-increase-forced-removals/deportations-at-the-heart-of-eu-migration-policy/databases-for-deportations/

Année	Initiative
2000	Adoption de la législation «Eurodac» exigeant l'enregistrement biométrique des demandeurs d'asile
2004	Approbation de la législation introduisant les passeports biométriques pour les citoyens de l'UE ; les ressortissants des pays qui ne requièrent pas de visa pour entrer dans l'UE doivent également posséder un passeport biométrique répondant aux mêmes normes
2006	Le système d'information Schengen de deuxième génération introduit des alertes biométriques en cas de refus d'entrée ou de séjour dans l'espace Schengen
2008	Approbation de la législation sur les titres de séjour biométriques pour les ressortissants étrangers
2008	Approbation de la législation sur les demandes de visas biométriques
2017	Approbation de la législation relative au système d'entrée/sortie, une base de données biométrique d'enregistrement d es passages frontaliers
2018	La nouvelle législation relative au système d'information Schengen rend obligatoire l'inclusion des décisions d'expulsion dans la base de données, qui peuvent inclure les empreintes digitales et les photographies.
2019	La législation sur «l'interopérabilité» est approuvée

Tableau 1 : Chronologie de la législation européenne en matière d'identification biométrique

De demandeurs d'asile à citoyens et résidents

Moins d'un an après l'adoption de la législation Eurodac initiale, l'UE a introduit de nouvelles normes de sécurité pour les permis de séjour[10] et les visas,[11] dans le but de prévenir la fraude d'identité et de documents. Toutefois, à ce moment-là, le contexte politique avait considérablement changé, à la suite des attentats du 11 septembre 2001 aux États-Unis et de l'avènement de la «guerre contre le terrorisme». Les normes de 2004 n'incluaient que les éléments de sécurité «traditionnels» - filigranes, hologrammes, etc. - et les gouvernements «ont clairement indiqué qu'ils [étaient] favorables à l'inclusion d'identifiants biométriques dans le visa et le titre de séjour des ressortissants de pays tiers afin d'établir un lien plus fiable entre le titulaire, le passeport et le visa».[12]

La Commission a répondu par un plan qui couvrait également les passeports des citoyens de l'UE : d'une part, pour répondre aux exigences américaines concernant les «éléments biométriques dans les passeports des citoyens des pays bénéficiant d'une exemption de visa à partir du 26 octobre 2004» et, d'autre part, pour atteindre l'objectif commun des États-Unis et de l'UE d'une «interopérabilité mondiale» dans l'utilisation de la biométrie «pour lutter contre le terrorisme et l'immigration illégale».[13] Dans le même temps, l'UE a financé un projet de recherche visant à soutenir «la mise en œuvre cohérente du passeport numérique européen de nouvelle génération».[14]

La législation exigeant l'ajout d'éléments biométriques aux passeports des citoyens de l'UE (une photographie et deux empreintes digitales) a été approuvée en 2004 ;[15] aux permis de séjour (deux empreintes digitales et une photographie) en avril 2008,[16] et aux visas de court séjour (dix empreintes digitales et une photographie) en juillet 2008.[17] Fin 2019, le «Système d'information sur les visas», une base de données contenant des données sur les demandes de visa Schengen de court séjour, pouvait contenir jusqu'à 100 millions de dossiers de visa, bien que le nombre réel détenu dans le système ne soit pas publié.[18] Dans le même temps, près de 20 millions de permis de séjour valides étaient en circulation. Les données sur le nombre de passeports biométriques des États membres de l'UE en circulation ne sont pas disponibles.

Les efforts en faveur de l'enregistrement biométrique des ressortissants étrangers ne se sont pas arrêtés là. En 2006, la législation améliorant le Système d'information Schengen (SIS) a été approuvée. Désormais, les signalements dans la base de données «émis à l'égard de ressortissants de pays tiers aux fins de non-admission et d'interdiction de séjour» peuvent contenir à la fois des empreintes digitales et des photographies, mais aussi une multitude d'autres informations.[19] En 2018, le système a encore été étendu, et les États membres sont désormais tenus d'ajouter les mesures d'éloignement (c'est-à-dire d'expulsion) dans la base de données. Comme pour les signalements de refus d'entrée ou de séjour, ceux-ci peuvent contenir des empreintes digitales et des photographies, aux côtés d'autres données personnelles.[20]

Après la mise à niveau du SIS en 2006, les politiciens, les fonctionnaires et les représentants du secteur ont commencé à vanter les mérites des «frontières intelligentes». En 2008, la Commission européenne a publié des propositions visant à numériser les contrôles aux frontières de l'UE. Celles-ci ont ensuite été retirées, avant d'être actualisées et réintroduites en 2013. Parmi celles-ci figurait une proposition de système d'entrée/sortie (*Entry/Exist System* EES), pour laquelle la législation a été approuvée en 2017.[21] L'EES sera utilisé pour enregistrer une photographie, quatre empreintes digitales et d'autres données de ressortissants étrangers qui n'ont pas besoin d'un visa pour entrer dans l'UE, dans le but de générer automatiquement des listes de personnes dépassant les limites de leur permis de séjour. L'objectif est de créer automatiquement des listes de ceux qui séjournent plus longtemps que prévu, afin d'aider les autorités à traquer et à expulser les «*overstayers*» (NdT : *c'est-à-dire une personne qui reste dans le pays, en infraction à la législation sur les étrangers, après que son autorisation de séjour a expiré*).

Vers l'interopérabilité

Au milieu des années 2010, l'UE exploitait, ou avait mandaté la construction, d'un ensemble de bases de données contenant des données biométriques pouvant être utilisées pour vérifier l'identité de ressortissants étrangers dans un large éventail de situations administratives différentes - des demandeurs d'asile aux résidents étrangers, en passant par les titulaires de visas et les migrants d'États non soumis à l'obligation de visa. Néanmoins, les fonctionnaires avaient un plan plus ambitieux en préparation : transformer les «silos» de données contenant ces informations en un système interconnecté, sous le nom de «interopérabilité».

Annonçant les propositions juridiques en décembre 2017, la Commission européenne a déclaré :

10 Règlement (CE) n° 1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32002R1030

11 du Conseil du 18 février 2002 modifiant le règlement (CE) n° 1683/95 établissant un modèle type de visa, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32002R0334

12 Commission européenne, «Proposal for a COUNCIL REGULATION amending Regulation (EC) 1683/95 laying down a uniform format for visas», 24 September 2003, https://www.statewatch.org/media/documents/news/2003/sep/combiometrics.pdf

13 Ambassade des États-Unis à Bruxelles, «BIOMETRICS : EU ON PARALLEL TRACK WITH U.S. AND MOVING FORWARD», 10 novembre 2004, https://search.wikileaks.org/plusd/cables/04BRUSSELS4844_a.html

14 https://cordis.europa.eu/project/id/507974

15 Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32004R2252

16 Règlement (CE) n° 380/2008 du Conseil du 18 avril 2008 modifiant le règlement (CE) n° 1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32008R0380

17 Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32008R0767

18 eu-Lisa, «Report on the technical functioning of the Visa Information System», August 2020, https://www.eulisa.europa.eu/Publications/Reports/2019%20VIS%20Report.pdf.

19 Chapitre IV, règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32006R1987#d1e1242-4-1

20 Article 4, «Catégories de données», Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1860#d1e783-1-1

21 Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 établissant un système d'entrée/sortie (SEE), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017R2226

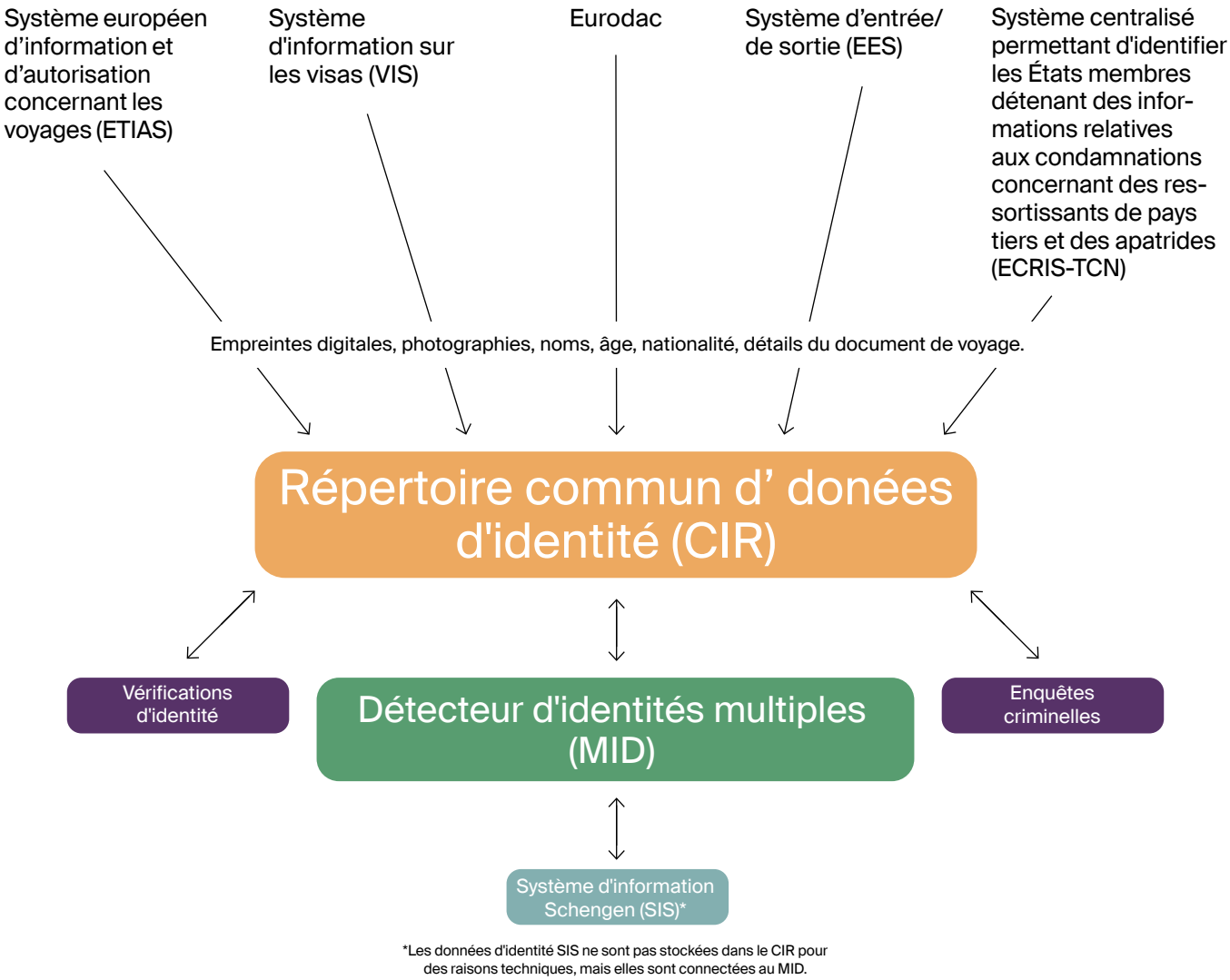


Figure 1 : Accès aux bases de données interopérables et interactions entre elles

> *«Au cours des trois dernières années, les menaces pour la sécurité intérieure ont évolué et sont encore très présentes, comme en témoignent la série d'attentats terroristes dans plusieurs États membres et l'augmentation des franchissements irréguliers des frontières extérieures de l'UE. Ces défis ont mis en évidence l'urgente nécessité de renforcer les outils d'information de l'UE en matière de sécurité, de gestion des frontières et des migrations».*[22]

Le directeur émérite de *Statewatch*, Tony Bunyan, a souligné le problème de cette justification en 2018 :

> *«La proposition de la Commission concernant les bases de données centralisées interopérables de l'UE est justifiée par la menace que représentent la migration et le terrorisme pour la sécurité intérieure. Cet amalgame de menaces fondé sur la peur de «l'autre» est un cas classique de racisme d'État institutionnalisé».*[23]

Le fait que le terrorisme et l'immigration n'aient que peu, voire rien à voir l'un avec l'autre n'a pas empêché les partisans de l'interopérabilité de poursuivre leurs efforts. Rien ne prouve non plus que les ressortissants étrangers constituent une menace plus importante pour la sécurité que les citoyens de l'UE, ce qui soulève la question de savoir si la pression en faveur de «l'interopérabilité» est exercée parce qu'elle est objectivement nécessaire ou simplement parce qu'elle est désormais techniquement possible.

L'impulsion initiale de ce plan est venue d'Allemagne, où les autorités ont créé un registre central des étrangers (*Ausländerzentralregister*) à la suite de la «crise migratoire» de 2015. Ce registre stocke un large éventail d'informations et son accès est étendu à une liste toujours plus longue d'autorités. Le projet de l'UE consiste à centraliser les «données d'identité» - photos, empreintes digitales, noms, nationalités et informations sur les documents de voyage - extraites de cinq bases de données européennes différentes à grande échelle.[24] Ces données seront placées dans un répertoire commun d'identité, appelé «Common Identity Repository» (CIR), et capable de contenir jusqu'à 300 millions enregistrements.[25] Ce système devrait officiellement entrer en

22 Commission européenne, « Frequently asked questions - Interoperability of EU information systems for security, border and migration management» , 12 décembre 2017, https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_17_5241

23 Tony Bunyan, «The point of no return», juillet 2018, p.14, https://www.statewatch.org/media/documents/analyses/no-332-eu-interop-morphs-into-central-database-revised.pdf

24 Eurodac, le Système d'entrée/sortie, le Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers, le Système européen d'information et d'autorisation concernant les voyages et le Système d'information sur les visas.

25 Daniel Trilling, «Scaled up surveillance : the EU builds a massive biometric database», Coda, 9 juin 2020, https://www.codastory.com/authoritarian-tech/eu-border-patrol-technology/

service l'année prochaine, bien que ce projet ambitieux ait connu des retards.[26,27]

Cette initiative vise notamment à faciliter les contrôles d'identité par les autorités répressives, dans le cadre de la lutte contre la fraude à l'identité mais aussi contribuer à l'augmentation du nombre d'expulsions.[28] L'accès au système sera autorisé en vertu de l'article 20 des règles d'interopérabilité, qui permet à «une autorité policière» d'effectuer des recherches en utilisant «les données biométriques de cette personne relevées en direct lors d'un contrôle d'identité, à condition que la procédure ait été engagée en présence de cette personne».[29] Le CIR sera également relié à un détecteur automatique d'identités multiples, qui effectuera des vérifications croisées à la recherche de données correspondantes chaque fois qu'un nouveau fichier sera créé dans une base de données de l'UE.

Le CIR sera accessible via des points d'accès fixes aux postes frontières, aux commissariats de police et aux consulats, entre autres, mais l'intention est également que les fonctionnaires utilisent le système via des technologies d'identification biométrique mobiles. Il s'agit habituellement d'appareils portatifs capables de capturer les données biométriques d'un individu (généralement son empreinte digitale ou son visage, bien qu'il existe d'autres moyens d'identification biométrique) et de les comparer automatiquement à une base de données ou à une liste de surveillance.

Il existe un marché important pour ces dispositifs, les entreprises, grandes et petites[30], étant désireuses de fournir aux autorités étatiques le dernier cri en matière d'outils d'identification individuelle. «Plus de 20 pays en Europe» utilisent du matériel produit par la société allemande DERMALOG, «pour des applications gouvernementales telles que l'enregistrement national, le contrôle des frontières et l'enregistrement des réfugiés».[31] Thales se targue de «plus de 200 déploiements biométriques dans 80 pays, tirant parti d'une authentification et d'une identification biométriques fortes dans le monde entier pour des clients à tous les niveaux de gouvernement» [32]. NEC affirme être «le premier fournisseur mondial de biométrie par empreintes digitales pour les applications de maintien de l'ordre et de gestion de l'identité», ayant passé «environ un demi-siècle à développer la technologie d'identification par empreintes digitales la plus efficace et la plus précise».[33]

Néanmoins, l'acquisition et l'utilisation des technologies biométriques mobiles sont considérées par la Commission européenne comme l'un des aspects les plus difficiles du projet d'interopérabilité : «La complexité attendue réside dans la nécessité pour les États membres d'acheter et de personnaliser des terminaux biométriques portables et de les connecter à leurs systèmes de police nationaux» [34], un processus qui exige des changements organisationnels et procéduraux substantiels (voir la section Réseaux de technologie policière du présent rapport).

Des modifications juridiques peuvent également être nécessaires afin d'adapter la législation nationale aux exigences de l'article 20, ce qui fait que, à l'été de l'année dernière, seuls 13 des États participant à l'initiative d'interopérabilité (moins de la moitié du total) avaient fini leur évaluation pour savoir si des modifications étaient nécessaires.[35]

Quant à l'acquisition de la technologie nécessaire pour intensifier les contrôles d'identité biométriques, il semble que la situation soit très différente d'un État à l'autre. Les demandes d'informations formulées dans le cadre de la loi sur la liberté de l'information et déposées par *Statewatch* pour l'établissement du présent rapport ont cherché à en établir l'état des lieux en France, en Italie et en Espagne, mais elles sont restées sans réponse. Parmi les experts de la société civile et les chercheurs interrogés par *Statewatch*, la connaissance des plans actuels est limitée, notamment en ce qui concerne la mise en œuvre de l'initiative d'interopérabilité.[36]

Malgré l'absence d'informations publiques complètes et accessibles sur la mise en œuvre, les dossiers indiquent néanmoins que les États prennent des mesures dans ce sens. En 2019, la police française a obtenu le pouvoir de vérifier, «à partir des empreintes digitales d'un étranger sans titre, s'il dispose ou non d'un titre enregistré dans l'AGDREF [Application de Gestion des Dossiers des Ressortissants Étrangers en France, soit le fichier des étrangers présents en France]».[37] L'administration a dépensé 7,5 millions € pour l'équipement de la base de données AGDREF et de différents types de lecteurs d'empreintes digitales depuis 2017, [38] et en février dernier, le Ministère de l'Intérieur a publié un appel à informations pour une «solution basée sur l'IA» permettant de croiser une identité dans plusieurs bases de données à partir d'une empreinte digitale. Il recherchait également des «solutions de capteurs biométriques» qui permettraient aux autorités de «répondre à de nouveaux besoins», notamment «la capture mobile des empreintes digitales… de préférence via un smartphone/tablette…e, voire à partir de l'appareil photo d'un smartphone/tablette».[39]

26 «UE : States slow to introduce legal changes easing biometric identity checks by police» , *Statewatch*, 18 juin 2021, https://www.statewatch.org/news/2021/june/eu-states-slow-to-introduce-legal-changes-easing-biometric-identity-checks-by-police/

27 Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 établissant un cadre pour l'interopérabilité entre les systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et des migrations, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32019R0818; Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 établissant un cadre pour l'interopérabilité entre les systèmes d'information de l'UE dans le domaine des frontières et des visas, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32019R0817

28 Conseil de l'UE, «Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area : - State of play of its implementation», 8 novembre 2016, https://www.statewatch.org/media/documents/news/2016/dec/eu-council-info-exhang-interop-sop-13554-REV-1-16.pdf

29 Article 20, «Accès au répertoire commun de données d'identité pour identification» , règlement 2019/818, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32019R0818#d1e1977-85-1

30 Aux côtés de DERMALOG, Thales et NEC, on trouve, entre autres, Bayometric, https://www.bayometric.com ; M2Sys, https://www.m2sys.com ; Idemia, https://www.idemia.com/morphoident ; HID Global, https://www.hidglobal.com/crossmatch ; et Coppernic, https://www.coppernic.fr/en

31 DERMALOG Fingerprint Scanners, *DERMALOG*, non daté, https://www.dermalog.com/products/hardware/fingerprint-scanners

32 Biométrie, *Thales*, non daté, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics

33 «Fingerprint Identification», *NEC*, non daté, https://www.nec.com/en/global/solutions/biometrics/fingerprint/index.html

34 Commission européenne, «Impact assessment», SWD(2017) 473 final Partie 2/2, p.51, https://www.statewatch.org/media/documents/news/2018/jan/eu-com-interoperability-swd-473-pt-2-17.pdf

35 «UE : States slow to introduce legal changes easing biometric identity checks by police», *Statewatch*, 18 juin 2021, https://www.statewatch.org/news/2021/june/eu-states-slow-to-introduce-legal-changes-easing-biometric-identity-checks-by-police/

36 Ateliers, «State databases, biometrics, policing and migration control», *Statewatch*, 7 et 14 octobre 2021, https://www.statewatch.org/projects/biometric-europe-civil-society-workshops/

37 «Interconnectivité des données biométriques entre les services de police», question écrite du 6 juillet 2017 et réponse du 28 mars 2019, Senat, https://www.senat.fr/questions/base/2017/qSEQ170700052.html

38 «Capteurs biométriques de lecteurs de documents d'identité et de voyage», *TED*, 10 avril 2019, https://ted.europa.eu/udl?uri=TED:NOTICE:170278-2019:TEXT:FR:HTML&src=0; « Fourniture de capteurs d'empreintes digitales et de lecteurs de cartes et prestation associée», *TED*, 26 septembre 2017, https://ted.europa.eu/udl?uri=TED:NOTICE:380656-2017:TEXT:FR:HTML&src=0 ; « Fourniture de capteurs d'empreintes digitales et de lecteurs de cartes et prestation associée», *TED*, 7 juin 2017, https://ted.europa.eu/udl?uri=TED:NOTICE:219264-2017:TEXT:FR:HTML&src=0

39 «Solutions de capteurs biométriques», *TED*, 26 février 2021, https://ted.europa.eu/udl?uri=TED:NOTICE:106736-2021:TEXT:FR:HTML&src=0

Ceci est déjà le cas en Allemagne : à Hambourg, une application mobile permet à la police de scanner les empreintes digitales à l'aide d'un smartphone.[40]
La police néerlandaise, quant à elle, fait figure de pionnière dans ce domaine. En 2011, les autorités ont commencé à fournir une technologie mobile de numérisation des empreintes digitales à la police, une mesure «principalement destinée à des contrôles plus intensifs des étrangers en situation irrégulière», selon le journal *Trouw*.[41] En Grèce, un programme financé par l'UE vise à équiper des centaines d'agents de scanners portables d'empreintes digitales et de visages dans le but de cibler les migrants en situation irrégulière.[42]

En 2014, les autorités espagnoles ont utilisé plus de 300 000 euros du Fonds pour la sécurité intérieure de l'UE pour équiper les agents de la *Guardia Civil* de «terminaux de données portables, avec lesquels il est possible d'accéder aux bases de données à distance et en temps réel», qui seront déployés «dans les zones présentant un risque élevé d'immigration irrégulière». Les autorités[43] [44] danoises[45] et suédoises ont également utilisé le Fonds de sécurité intérieure pour acheter des dispositifs d'identification mobiles afin de faciliter la mise en œuvre du système d'entrée/sortie, tandis que les autorités roumaines ont acheté des «dispositifs de contrôle mobiles» pour faciliter l'accès au système d'information Schengen.[46]

Il semble donc y avoir un patchwork de différentes initiatives nationales sur l'identification mobile, dont certaines sont liées à la mise en œuvre et à l'utilisation des bases de données de l'UE, et d'autres non. Cependant, une fois que les dispositifs d'identification biométrique mobiles sont utilisés, ils peuvent être connectés à d'autres systèmes et sources de données. Il existe sans aucun doute d'autres projets et déploiements que ceux qui ont été découverts au cours des recherches menées dans le cadre du présent rapport, et il y en aura probablement beaucoup d'autres à venir au fur et à mesure de la mise en œuvre de l'initiative d'interopérabilité et des plans nationaux visant à accroître les contrôles biométriques mobiles. Il est nécessaire d'enquêter davantage sur ces projets et de les examiner de plus près, afin de s'assurer que les autorités respectent, à tout le moins, leurs obligations de réaliser des évaluations d'impact significatives en matière de non-discrimination et de protection des données, et de mettre en place des garanties adéquates concernant les contrôles d'identité effectués par la police et les services d'immigration.

40 Franziska Rau, «Polizei Hamburg scannt Fingerabdrücke jetzt auch per Handy», *Netzpolitik*, 5 novembre 2021, https://netzpolitik.org/2021/mobipol-polizei-hamburg-scannt-fingerabdruecke-jetzt-auch-per-handy/

41 «Politie neemt vingerafdruk af op straat», *Trouw*, 20 juillet 2011, https://www.trouw.nl/nieuws/politie-neemt-vingerafdruk-af-op-straat~bee8d48a/

42 «Grèce : New Biometrics Policing Program Undermines Rights», *Human Rights Watch*, 18 janvier 2022, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

43 «Adquisición de equipamiento ámbito del programa de movilidad en lucha inmigración ilegal», *Open Security Data Europe*, https://opensecuritydata.eu/projects/Acquisition-of-equipment-within-the-scope-of-the-mobility-program-in-the-fight-against-illegal-immig--106.

44 «Acquisition of hardware/equipment for implementation of the regulation for a entry and exit system (ESS) in the police», *Open Security Data Europe*, https://opensecuritydata.eu/projects/Acquisition-of-hardwareequipment-for-implementation-of-the-regulation-for-a-entry-and-exit-system-(E--119).

45 «Upphandling av mobil fingeravtryckskläsare för gränskontroll», *Open Security Data Europe*, https://opensecuritydata.eu/projects/Procurement-of-mobile-fingerprint-reader-for-border-control

46 «Modernizare SIS recast PFR», *Open Security Data Europe*, https://opensecuritydata.eu/projects/Modernization-of-SIS-recast-PFR

Les demandeurs d'asile : des cobayes pour «l'interopérabilité».

Ces dernières années, l'État espagnol a considérablement développé ses systèmes biométriques. À leur arrivée aux frontières espagnoles, les personnes demandant l'asile voient leurs informations enregistrées dans un «système intégral de gestion des demandes de protection internationale», ou SIGESPI. Ce système est géré par la société GMV.[47] Ironiquement, cette société est également responsable de la gestion du système européen de surveillance des frontières, EUROSUR[48], conçu en partie pour tenter d'éloigner les demandeurs d'asile du territoire de l'UE. [49]

Démontrant la tendance à «l'interopérabilité» au niveau national, le système est connecté à une multitude d'autres bases de données, dont celles de la police, des casiers judiciaires, de l'état civil et des visas, afin de vérifier les antécédents des demandeurs d'asile. L'organisation de défense des droits humains *Novact* a noté que «la centralisation et l'interopérabilité entre les bases de données présentent de graves risques pour la vie privée des personnes».[50] Que ce soit au niveau local, national, régional ou international, plus les données sont interconnectées et plus les points d'accès sont nombreux, plus il est probable que les données soient consultées et utilisées illégalement, en particulier si les autorités de protection des données chargées de la supervision et de l'inspection ne disposent pas des ressources nécessaires pour mener à bien leurs tâches.

En effet, la gendarmerie espagnole, la *Guardia Civil*, a systématiquement eu accès (et de manière illégale) au SIGESPI entre 2013 et 2014 à des fins d'enquêtes criminelles, enregistrant quelque 1,5 million de recherches sur cette période. Cette pratique a été dénoncée en 2015 par la *Policía Nacional*, qui contrôle le système.[51] Accorder aux forces de police l'accès aux systèmes détenant des données sur les demandeurs d'asile et autres ressortissants étrangers à des fins d'enquêtes criminelles est désormais une pratique courante au niveau de l'UE, suite à l'adoption de modifications controversées d'Eurodac en 2013.[52] Dans la pratique, cela a pour effet de criminaliser ces groupes : s'il n'existe pas de bases de données similaires stockant des informations recueillies auprès des citoyens, il est impossible de les soumettre au même niveau d'examen policier.

En outre, le nombre croissant d'autorités autorisées à accéder aux systèmes nationaux et européens augmente les possibilités d'accès illégal aux données, que ce soit au niveau individuel ou institutionnel. Bien que la législation contienne généralement des garanties exigeant le contrôle et l'enregistrement de l'accès aux données, le respect de ces dispositions implique une charge de travail considérablement accrue pour les autorités nationales chargées de la protection des données, dont bon nombre manquent déjà de ressources et de personnel. La complexité juridique et pratique des systèmes interopérables aggrave encore le problème.

47 «Vulneraciones de derechos humanos en las deportaciones», *Irídia/Novact*. 2020, p.118, https://novact.org/wp-content/uploads/2020/10/Deportaciones2.pdf

48 «Poland-Warsaw : Single Framework Contract for the provision of ICT products and services for Eurosur», https://ted.europa.eu/udl?uri=TED:NOTICE:391665-2018:TEXT:FR:HTML&src=0

49 Charles Heller et Chris Jones, «Eurosur : saving lives or reinforcing deadly borders ?», *Statewatch*, 1er février 2014, https://www.statewatch.org/statewatch-database/eurosur-saving-lives-or-reinforcing-deadly-borders-by-charles-heller-and-chris-jones/

50 «Vulneraciones de derechos humanos en las deportaciones», *Irídia/Novact*. 2020, p.118, https://novact.org/wp-content/uploads/2020/10/Deportaciones2.pdf

51 Luís Durán, «Guerra de agentes por un millón de datos», *El Mundo*, 22 juin 2015, https://www.elmundo.es/espana/2015/06/22/5585b6afe2704ef8328b4575.html

52 «Common European Asylum System : Council adopts the Eurodac regulation», *Statewatch*, 21 juin 2013, https://www.statewatch.org/news/2013/june/eu-eurodac-council-of-the-european-union-common-european-asylum-system-council-adopts-the-eurodac-regulation/

3.

Financement des technologies biométriques

L'UE est l'un des plus grands pourvoyeurs de fonds publics pour la «recherche et l'innovation» dans le monde, et des sommes importantes ont été consacrées au développement des technologies nécessaires à la mise en œuvre de son programme d'identité biométrique. Le programme de recherche actuel de l'UE, «Horizon Europe», court de 2021 à 2027 et dispose d'un budget total d'environ 95 milliards € .[53] Il permettra de financer des projets et des activités dans les domaines de la recherche médicale, de l'environnement, du changement climatique et des transports, entre autres. Un segment du programme, d'une valeur de 1,6 milliard €, est consacré à la sécurité, sous le titre «Sécurité civile pour la société».

Biométrie et recherche sur la sécurité

Le thème de la sécurité civile pour la société est la dernière itération du programme européen de recherche sur la sécurité, qui existe depuis 2004 et qui a été formellement intégré dans le programme de recherche plus large à partir de 2007. Il est axé sur le développement de nouvelles technologies et techniques pour faire face à des problèmes tels que la criminalité, le terrorisme, le contrôle des frontières, la gestion et la réaction aux catastrophes et la cybersécurité. Pour ce faire, il finance principalement les activités de consortiums - composés d'entreprises privées, d'organismes publics, d'instituts de recherche ou d'établissements d'enseignement supérieur - qui sont formés spécialement pour mener à bien des projets de recherche particuliers.

Dans le domaine de la sécurité, ces recherches ont porté, par exemple, sur le développement de nouvelles techniques de vidéosurveillance, sur des[54] réseaux de différents capteurs pouvant être montés sur des drones et utilisés pour le contrôle des frontières,[55] ou bien sur des outils de communication pour les services d'urgence.[56] Les autorités nationales ont souvent aussi leurs propres programmes de recherche en matière de sécurité - par exemple, le gouvernement allemand a financé des recherches visant à développer «une solution technique permettant l'authentification de l'identité pour une utilisation mobile par la police et les autorités compétentes».[57]

La technologie biométrique est depuis longtemps au cœur du programme de recherche sur la sécurité, même si le financement de la recherche européenne dans ce domaine remonte à bien plus loin. À la fin des années 1990 et au début des années 2000, le financement de la biométrie provenait en grande partie du volet consacré aux technologies de l'information des 5é et 6è Programme-cadre de recherche (1998-2002 et 2002-2006, respectivement) et était orienté vers de potentielles applications commerciales ou de santé.

À partir de 2007, cependant, le thème de la sécurité est devenu de loin la source la plus importante de ce financement, et le nombre de projets financés est monté en flèche - ce qui démontre clairement le rôle central accordé à l'identité biométrique dans le programme de sécurité de l'UE. Au total, depuis 1998, l'UE a accordé plus de 290 millions € de fonds publics à des projets de recherche et de développement dans le domaine de la biométrie. Près de 40% de ces projets concernaient principalement des questions de «sécurité publique» - application de la loi, contrôle des frontières et autres sujets similaires.[58] Les projets ont examiné les utilisations génériques de la technologie (par exemple, «une technologie innovante pour prendre des images d'empreintes digitales» ou des systèmes pour tester et certifier différents systèmes biométriques) ainsi que les utilisations appliquées de la biométrie, en particulier dans le domaine du contrôle des frontières.

53 Commission européenne, «What is Horizon Europe ?», https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

54 P-REACT, CORDIS, https://cordis.europa.eu/project/id/607881

55 «High-tech sensors to streamline EU border surveillance», CORDIS, https://cordis.europa.eu/article/id/175094-high-tech-sensors-to-streamline-eu-border-surveillance

56 «Towards next-generation emergency communication networks», CORDIS, https://cordis.europa.eu/article/id/147267-towards-nextgeneration-emergency-communication-networks

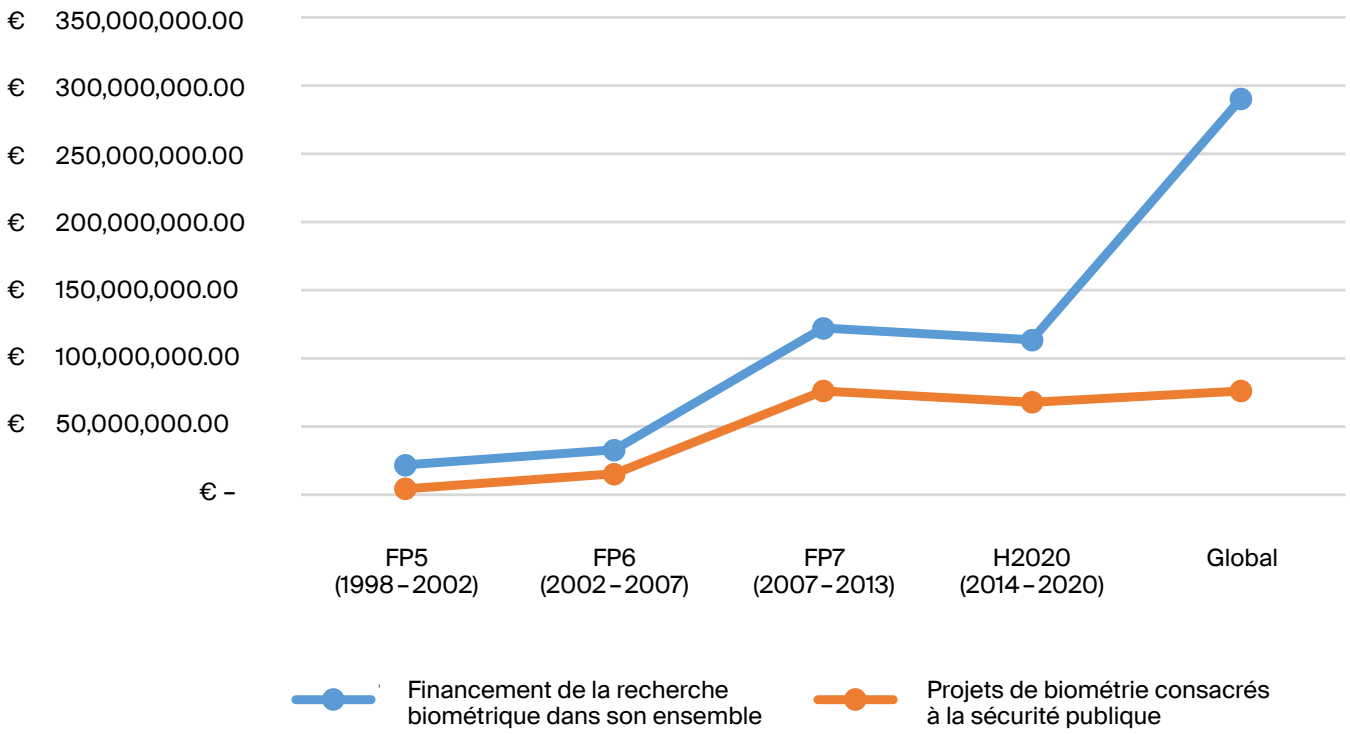
57 «Mobile Contactless Identity Verification in the Application Field of Migration», MEDIAN, https://blog.hwr-berlin.de/MEDIAN/en/about-median/

58 Tous les chiffres fournis dans cette section sont basés sur une analyse des données CORDIS disponibles sur le portail de données ouvertes de l'UE, https://data.europa.eu/euodp/en/data/

	Financement total de la biométrie	**Nombre total de projets**	**Financement de la biométrie de sécurité**	**Nombre de projets de sécurité**	**Dépenses de sécurité, en% du total**
Horizon 2020 (2014-20)	€113 547,610	57	€67 810,015	27	60%
FP7 (2007-13)	€122 127,732	27	€76 108,539	11	62%
FP6 (2002-2006)	€32 843,791	13	€15 249,995	4	46%
FP5 (1998-2002)	€21 828,594	16	€4 295,966	4	20%
Total	**€290 347,735**	**113**	**€163 464,515**	**46**	**56%**

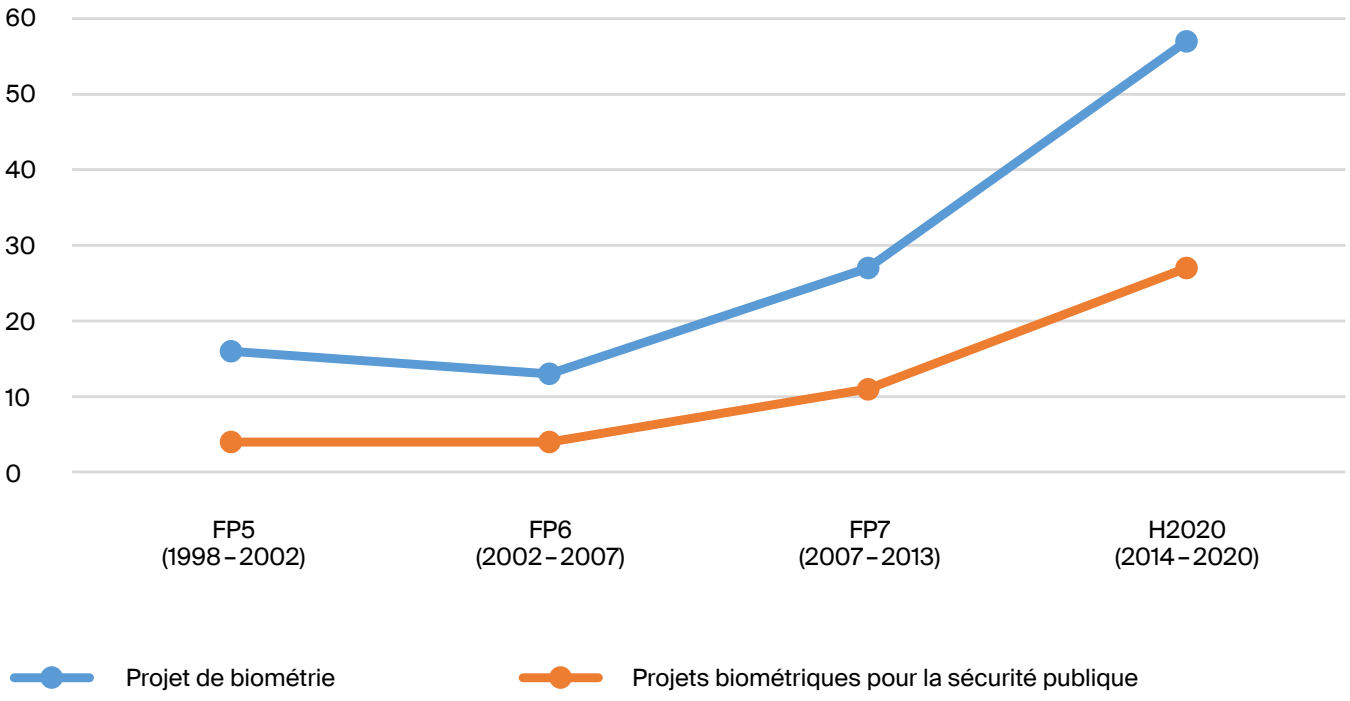
Tableau 2 : Financement consacré à la biométrie dans les programmes de recherche de l'UE, 1998-2020

Financement consacré à la biométrie dans les programmes de recherche de l'UE, 1998-2020



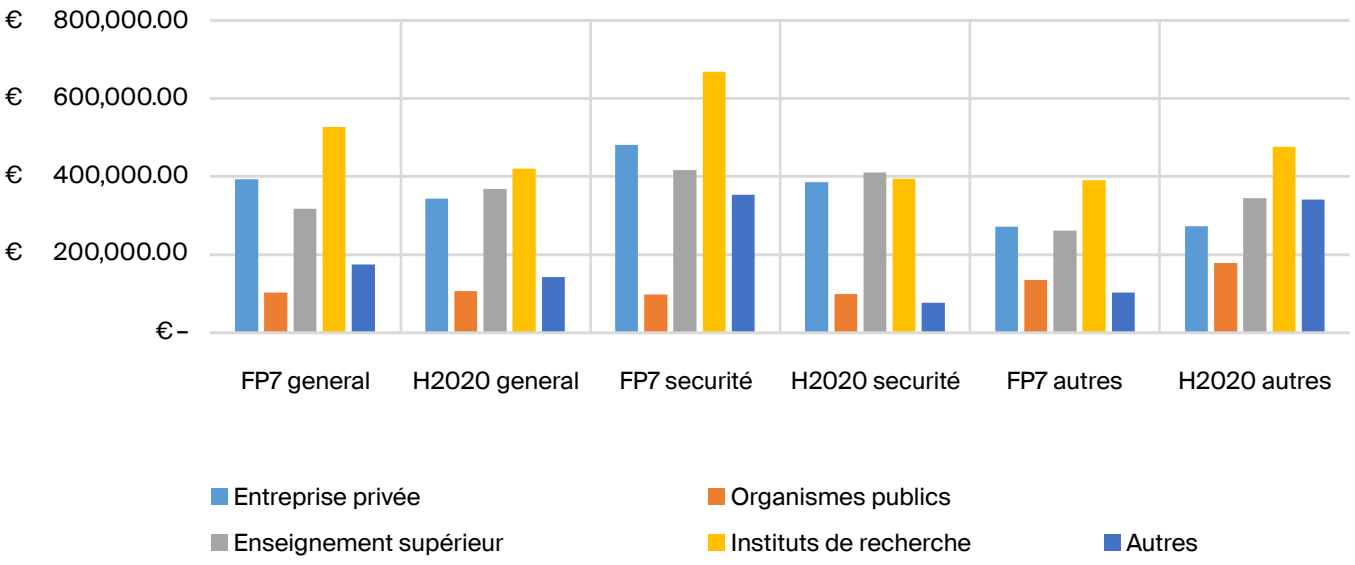
Graphique 1 : Financement consacré à la biométrie dans les programmes de recherche de l'UE, 1998-2020
Ce graphique montre les montants consacrés à la recherche biométrique dans son ensemble, ainsi que le montant consacré à la recherche des projets liés à la sécurité publique.

Nombre de projets de recherche financés par l'UE dans le domaine de la biométrie, 1998-2020



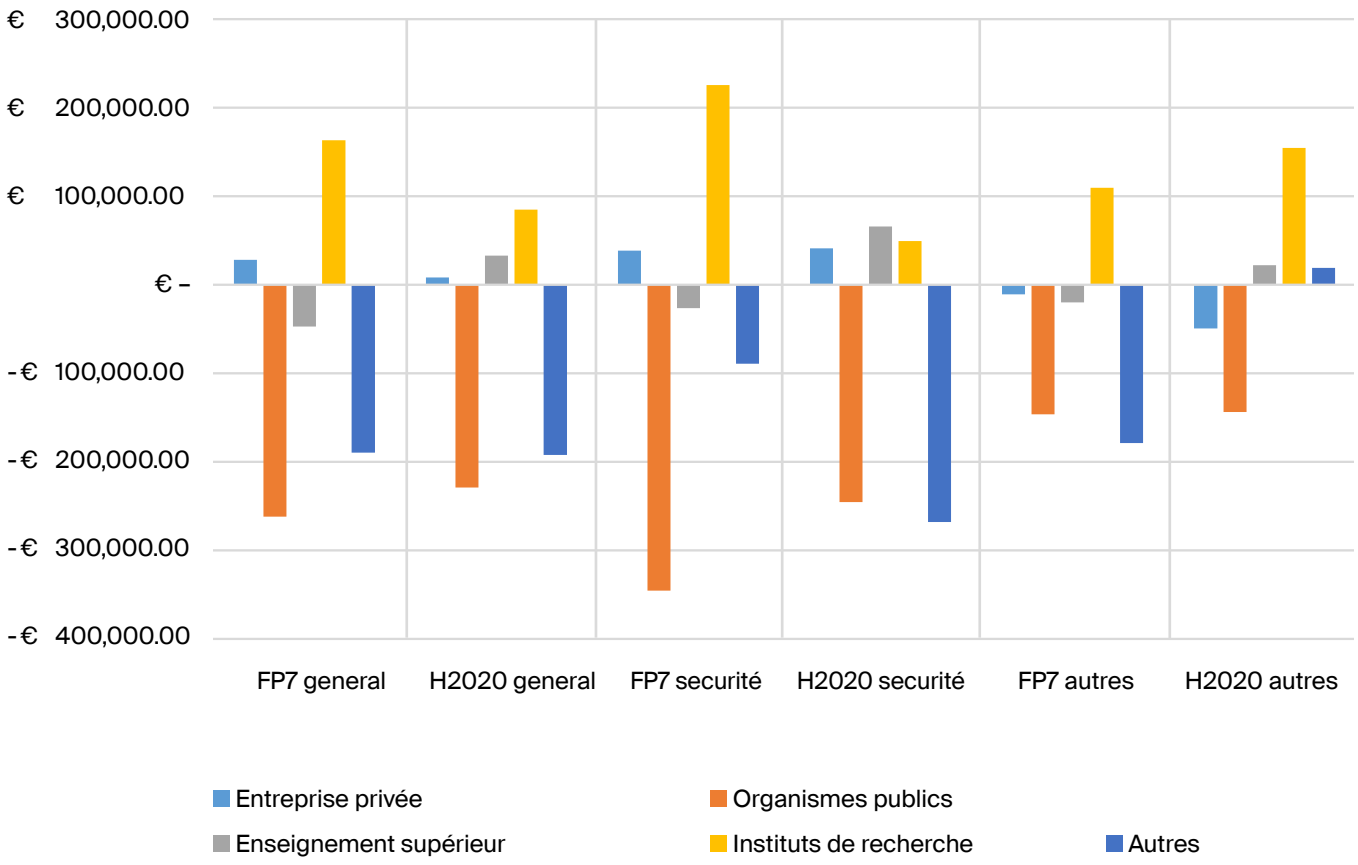
Graphique 2 : Nombre de projets de recherche biométrique financés par l'UE, 1998-2020.
Ce graphique montre le nombre de projets consacrés à la recherche sur la biométrie dans son ensemble, et le nombre de projets liés à la sécurité publique.

Financement moyen par projet de recherche biométrique par type d'institution, FP7 et H2020



Graphique 3 : Financement moyen par projet de recherche biométrique par type d'institution, FP7 et H2020. Ce graphique montre que le montant moyen du financement reçu par les entreprises privées, les établissements d'enseignement supérieur et les instituts de recherche a toujours été plus élevé pour les projets de sécurité publique que pour les autres types de projets de recherche en biométrie.

Différence entre la moyenne reçue par projet, par rapport au financement moyen global par projet



Graphique 4 : Différence entre la moyenne reçue par projet, par rapport au financement moyen global par projet. Ce graphique montre si les différents types d'institutions ont reçu plus ou moins de financement des programmes de recherche FP7 et H2020 par rapport au montant moyen accordé (la moyenne est représentée par la ligne centrale marquée €-). Par exemple, les organismes publics ont toujours reçu beaucoup moins que la moyenne, et les entreprises privées ont toujours reçu plus que la moyenne pour leur participation à des projets de sécurité publique.

Sur les 27 projets de recherche biométrique financés entre 2007 et 2013, 11 (41%) faisaient partie du programme de recherche sur la sécurité. Cette proportion a augmenté dans le cadre de «Horizon 2020», où 27 des 57 projets de recherche biométrique (47%) relevaient de la sécurité. Les projets axés sur la sécurité ont également reçu davantage de fonds que ceux qui recherchent des moyens de déployer la biométrie dans d'autres domaines : au cours du 7e Programme-cadre, les projets de sécurité ont reçu 43% des fonds consacrés à la biométrie ; dans la période de «Horizon 2020», cette part est passée à 60%.

Promouvoir les intérêts de l'État et de l'industrie

Les entreprises privées, ainsi que les instituts de recherche et les établissements d'enseignement supérieur soutenus par l'État, ont été les principaux bénéficiaires financiers de la recherche en biométrie, un fait qui est particulièrement prononcé dans le programme de recherche sur la sécurité. Les entreprises privées ont reçu près de 53 millions € (43%) du financement total de la recherche en biométrie dans le 7e Programme-cadre, mais ce chiffre est passé à 49% du financement accordé dans le cadre du thème de la sécurité (37,5 millions €). En revanche, ils n'ont reçu que 34% du financement (15,4 millions €) accordé à la recherche en biométrie dans le cadre d'autres thèmes. Dans le cadre d'Horizon 2020, le tableau est similaire : les entreprises privées ont reçu 49% de l'ensemble des fonds alloués à la recherche biométrique (55,6 millions €). Ce montant est passé à 57% (38,9 millions €) pour le volet sécurité, mais a chuté à 36% du financement accordé (16,6 millions €) pour les autres volets de recherche.

Un petit nombre de ces projets de recherche ont cherché à étudier les implications éthiques et juridiques des technologies biométriques pour le maintien de l'ordre et le contrôle des frontières.[59] Toutefois, la grande majorité d'entre eux visaient à trouver de nouveaux moyens et modes d'identification et d'authentification biométriques (y compris la reconnaissance[60] de la démarche et l'analyse[61] de la parole, en plus de la reconnaissance plus «traditionnelle» du visage et des empreintes digitales), ainsi que des moyens plus efficaces pour les autorités de les utiliser. Il convient également de noter que même si un projet de recherche est

59 «Privacy, ethical, regulatory and social no-gate crossing point solutions acceptance», *CORDIS*, https://cordis.europa.eu/project/id/787123 ; «Rising pan-European and International Awareness of Biometrics and Security Ethics», *CORDIS*, https://cordis.europa.eu/project/id/230389 ; «Biometric identification technology ethics promoting research and public debate on bioethical implications of emerging biometric identification technologies», *CORDIS*, https://cordis.europa.eu/project/id/6093.

60 «Gait Biometrics 3», *CORDIS*, https://cordis.europa.eu/project/id/662784

61 «LipVerify», *CORDIS*, https://cordis.europa.eu/project/id/728649

Pays	H2020	FP7	Total
Royaume-Uni	€17 249 314	€ 9 326 356	€26 575 671
Espagne	€15 536 605	€10 556 553	€26 093 158
Allemagne	€12 833 926	€12 863 261	€ 25 697 187
France	€9 307 630	€12 834 126	€22 141 755
Italie	€7 668 215	€11 691 939	€19 360 154
Grèce	€8 120 425	€5 774 133	€13 894 558
Pays-Bas	€4 074 005	€5 316 198	€9 390 204
Belgique	€5 061 878	€3 785 362	€8 847 240
Autriche	€4 513 025	€3 477 791	€7 990 816
Finlande	€1 137 943	€6 734 474	€7 872 416
Norvège	€4 782 978	€2 497 570	€7 280 548
Suisse	€2 025 986	€4 981 970	€7 007 956
Portugal	€3 322 625	€2 767 006	€6 089 631
Roumanie	€2 003 408	€3 245 933	€5 249 341
Pologne	€2 438 817	€2 418 245	€4 857 063
Suède	€979 958	€3 555 097	€4 535 055
Danemark	€2 690 857	€ -	€2 690 857
Irlande	€1 580 126	€1 078 372	€2 658 498
Islande	€1 405 750	€1 164 620	€2 570 370
USA	€ -	€2 321 915	€2 321 915

Tableau 3 : Répartition du financement de la recherche biométrique par État (20 premiers)

ostensiblement orienté vers l'utilisation de la biométrie à des fins commerciales, sanitaires ou autres fins plus «bénignes» que le maintien de l'ordre ou l'immigration, il est toujours conçu pour favoriser l'utilisation de techniques avancées de traitement des données et de surveillance, et la technologie de base elle-même peut très bien être adaptée à d'autres fins.

On peut toutefois se demander dans quelle mesure le programme de recherche sur la sécurité lui-même est un succès. Le programme est censé contribuer au développement, à l'essai, à l'acquisition et au partage de technologies, de techniques, de connaissances et de produits, dans le but de stimuler l'industrie européenne de la sécurité et, en fin de compte, d'assurer «une sécurité accrue des citoyens européens». Cependant, les évaluations officielles du 7e Programme-cadre et de H2020 ont fait état d'un faible nombre d'enregistrements de propriété intellectuelle et de publications universitaires ; et l'évaluation intermédiaire de H2020 a noté que «les membres du consortium peuvent être réticents à céder leur [propriété intellectuelle] pour permettre la commercialisation du produit final».[62] Le rapport cite ensuite un exemple :

> *«Les utilisateurs finaux [c'est-à-dire les gardes-frontières] expliquent que les contribuables européens paient mais n'obtiennent au final qu'un produit de démonstration ou un prototype à la fin du projet, avec une adoption limitée, voire nulle. Dans le cadre d'un projet, tant FRONTEX que les agences frontalières nationales auraient aimé utiliser la technologie, mais on leur a demandé 150 000 € pour pouvoir utiliser la plateforme».*[63]

Néanmoins, l'UE a clairement joué un rôle dans l'établissement et le maintien de réseaux collaboratifs de petites et grandes entreprises, d'établissements de recherche et d'enseignement et d'autorités publiques travaillant au développement et au déploiement de nouvelles technologies d'identification et de vérification biométriques. Ceci devrait se poursuivre dans la dernière itération du programme de recherche sur la sécurité : le programme de travail 2021-22 comprend des sujets sur «les biométries modernes utilisées en médecine légale et par la police» ; «l'amélioration des contrôles aux frontières pour faciliter les voyages aux frontières extérieures et l'amélioration des expériences» ; et «le renforcement de la sécurité et la lutte contre les fraudes en matière de gestion de l'identité et de documents d'identité et de voyage».[64]

62 Commission européenne, « Interim evaluation of the activities under the secure societies challenge under Horizon 2020 «, juillet 2017, https://op.europa.eu/en/publication-detail/-/publication/b8d4d47e-9db0-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-42979546, p.54.

63 Ibid.

64 Le programme de travail est disponible ici : «EU : €5 million for new wiretapping technologies», *Statewatch*, 25 août 2021, https://www.statewatch.org/news/2021/august/eu-5-million-for-new-wiretapping-technologies/

Institution	Financement du FP7	Financement H2020	Financement total
Idemia Identity & Security (France)	€7 194 528	€2 259 944	€9 454 471
Institut Fraunhofer (Allemagne)	€5 502 548	€2 683 323	€8 185 870
Institut autrichien de technologie	€4 332 493	€666 919	€4 999 412
Vision Box (Portugal)	€2 552 437	€2 093 700	€4 646 137
Université catholique de Louvain (Belgique)	€3 091 779	€1 329 280	€4 421 059
Université de Reading (UK)	€1 430 943	€2 515 304	€3 946 247
Institut des technologies de l'information (Grèce)	€3 032 426	€818 871	€3 851 297
Institut de recherche Idiap (Suisse)	€2 859 079	€562 553	€3 421 632
Université de Lancaster (UK)	€376 276.91	€2 953 573.15	€3 329 850 06
Atos (Espagne)	€1 932 744.18	€1 194 166.88	€3 126 911.06
Institut de recherche sur la défense (Suède)	€2 933 183.50	€-	€2 933 183.50
Veridos (Allemagne)	€417 705.50	€2 324 075.00	€2 741 780.50
Commissariat aux énergies alternatives et à l'énergie atomique (France)	€1 443 370.00	€1 223 807.50	€2 667 177.50
Thales (France)	€2 097 342.70	€474 936.25	€2 572 278.95
Collège universitaire de Gjøvik (Norvège)	€2 396 193.00	€-	€2 396 193.00
EURECOM (France)	€646 175.00	€1 717 632.83	€2 363 807.83
Université autonome de Madrid (Espagne)	€1 314 584.00	€1 003 619.52	€2 318 203.52
Zwipe (Norvège)	€-	€2 297 400.00	€2 297 400.00
Indra (Espagne)	€1 991 201.37	€222 250.00	€2 213 451.37

Tableau 4 : Les 20 principaux bénéficiaires du financement de la recherche biométrique, FP7 (2007-13) et H2020 (2014-20)

Des liens plus étroits sont également tissés avec les «utilisateurs finaux» prévus de ces nouvelles technologies. L'agence européenne chargée des frontières, Frontex, a joué un rôle accru dans le programme à la suite de l'entrée en vigueur de son mandat pour 2019. L'année dernière[65], elle a commandé une étude sur «la biométrie pour l'avenir des voyages», afin de contribuer à la définition des priorités de recherche.[66] Un mandat renouvelé pour l'agence de police Europol est également en préparation, qui lui permettra «d'aider la Commission à identifier les principaux thèmes de recherche, à élaborer et à mettre en œuvre les programmes-cadres de l'Union pour la recherche et l'innovation qui sont pertinents pour les objectifs d'Europol».[67] Un plus grand contrôle public et démocratique du programme de recherche, qui a longtemps cherché à avant tout propulser les intérêts des agences gouvernementales et des entreprises,[68] est nécessaire pour faire contrepoids.

65 Frontex, «Frontex to provide border security expertise to European Commission's research projects», 6 février 2020, https://frontex.europa.eu/media-centre/news/news-release/frontex-to-provide-border-security-expertise-to-european-commission-s-research-projects-ZrCBoM

66 Frontex, «New Research Study : Technology Foresight on Biometrics for the Future of Travel», 18 février 2021, https://frontex.europa.eu/media-centre/news/news-release/new-research-study-technology-foresight-on-biometrics-for-the-future-of-travel-ugObkJ

67 Considérant 11, Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEILmodifiant 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 personnel par Europol à l'appui des enquêtes pénales, et le rôle d'Europol en matière de recherche et d'innovation, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52020PC0796

68 Voir «Market Forces» (https://statewatch.org/marketforces) et «NeoConOpticon» (https://www.statewatch.org/publications/reports-and-books/neoconopticon-the-eu-security-industrial-complex), *Statewatch/Transnational Institute.*

	Entreprises privées		**Organismes publics**		**Établissements d'enseignement supérieur**		**Instituts de recherche**		**Autre**		**Total en €**
	Montant en €	**% du total**	**Montant en €**	**% du total**	**Montant en €**	**% du total**	**Montant en €**	**% du total**	**Montant en €**	**% du total**	
Total FP7	52 966 852	43	€2 968 732	2	32 665 983	27	32 150 973	26	1 220 495	1	**121 973 034**
Total H2020	55 573 383	49	3 397 837	3	36 787 747	32	17 217 923	15	570 730	1	**113 547 619**
Sécurité du FP7	37 534 411	49	2 428 208	3	15 400 855	20	20 038 662	26	706 403	1	**76 108 539**
Sécurité H2020	38 928 437	57	2 862 799	4	14 767 350	22	11 021 949	16	229 480	0	**67 810 015**
FP7 autres	15 432 441	34	540 524	1	17 265 128	38	12 112 311	26	514 092	1	**45 864 495**
H2020 autres	16 644 945	36	535 038	1	22 020 397	48	6 195 974	14	341 250	1	**45 737 604**

Tableau 5 : Financement européen de la recherche sur les technologies biométriques dans le cadre du FP7 (2007-2013) et du programme H2020 (2014-20)

Financement des «frontières intelligentes

C'est par le biais du programme de recherche et développement du 7e Programme-cadre que l'UE a cherché à développer la technologie nécessaire à son initiative de «frontières intelligentes» : des projets tels que ABC4EU[69], FASTPASS[70], FIDELITY[71] et MOBILEPASS[72] ont oeuvré au développement de portiques de contrôle automatisés aux frontières et de technologies d'acquisition et de vérification biométriques rapides, fiables et mobiles. L'évaluation globale la plus récente du programme de recherche a souligné que le projet MOBILEPASS était une réussite :

> «L'équipement mis au point permet aux autorités de procéder à l'acquisition d'empreintes digitales sans contact, ce qui englobe toute la chaîne allant des données d'empreintes digitales obtenues à partir des passeports jusqu'à la vérification sans contact. Cette solution innovante présente également une importante valeur ajoutée, car les contrôles aux frontières peuvent être exécutés de manière plus confortable, rapide et sûre».[73]

L'État espagnol a adopté avec enthousiasme les nouvelles technologies biométriques aux frontières, grâce à des fonds provenant de divers budgets européens et nationaux.[74] Le pays s'est montré particulièrement intéressé par les «frontières intelligentes» qui sous-tendront le système d'entrée/sortie, dans lequel toutes les personnes voyageant pour affaires, vacances et autres raison entrants dans l'UE verront leurs données biométriques stockées et leurs passages aux frontières enregistrés. Le projet ABC4EU (Automated Border Control Gates for Europe, soit le contrôle automatisé des frontières), d'un montant de 18 millions €, a été coordonné par la société de sécurité espagnole *Indra*, et cinq des 18 participants au projet sont basés en Espagne.[75] Les portiques ABC peuvent utiliser la reconnaissance faciale, la reconnaissance de l'iris, les empreintes digitales ou d'autres caractéristiques biométriques pour faire correspondre les informations d'une personne soit à son document de voyage, soit aux données enregistrées dans une base de données centrale, voire aux deux. Ironiquement, malgré les affirmations des défenseurs des systèmes ABC selon lesquelles ils garantiront la commodité et la rapidité des passages aux frontières, un projet pilote initial mené en 2015 à la frontière entre l'Espagne et Gibraltar a entraîné des files d'attente si importantes qu'il a été interrompu au bout de deux heures.[76] Les portiques constitueront toutefois un site clé pour la collecte et la vérification des données biométriques et autres. Cette même frontière a récemment accueilli un essai du système d'échange d'informations électroniques soutenu par Frontex, qui a annoncé que le système «changera la façon dont nous traversons les frontières et contribuera à protéger la sécurité des citoyens européens en centralisant [sic] les informations sur le passage des frontières».[77] L'entreprise *Everis* recevra près de 6,4 millions € pour construire le système national espagnol et le connecter à la base de données centrale du SEE.[78] Un appel d'offres de 20 millions € pour la fourniture d'équipements aux points de passage frontaliers espagnols a été clos à la fin de l'année dernière.[79]

69 «ABC Gates 4 Europe», *CORDIS*, https://cordis.europa.eu/project/id/312797

70 «A harmonized, modular reference system for all European automated border crossing points», CORDIS, https://cordis.europa.eu/project/id/312583

71 «Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy», CORDIS, https://cordis.europa.eu/project/id/284862

72 «A secure, modular and distributed mobile border control solution for European land border crossing points », CORDIS, https://cordis.europa.eu/project/id/608016

73 Commission européenne, «Interim evaluation of Horizon 2020 – Annex 2», 29 mai 2017, https://ec.europa.eu/info/publications/annexes-1-and-2-interim-evaluation-horizon-2020_en

74 «Vulneraciones de derechos humanos en las deportaciones», *Irídia/Novact*, 2020, pp.112-3 https://novact.org/wp-content/uploads/2020/10/Deportaciones2.pdf

75 «ABC Gates 4 Europe, CORDIS, https://cordis.europa.eu/project/id/312797

76 «Gibraltar culpa a la frontera inteligente de provocar colas», *EuropaSur*, 28 juillet 2015, https://www.europasur.es/gibraltar/Gibraltar-frontera-inteligente-provocar-colas_0_938906484.html

77 «Frontex Entry Exit System Pilot Project», 5 novembre 2021, https://frontex.europa.eu/media-centre/news/news-release/frontex-entry-exit-system-pilot-project-6FimQn

78 «Contratación de un sistema completo, software, hardware y los desarrollos necesarios para su explotación, con la finalidad de proceder a la implementación del nuevo sistema de registro electrónico de entradas y salidas y su conexión al sistema central del EES (proyecto entry / exit system, EES)», *Plataforma del Contratación del Sector Público*, https://contrataciondelestado.es/wps/wcm/connect/1defb279-5e6f-4db8-bec6-dafa82c4d645/DOC_FORM2021-688548.html?MOD=AJPERES

79 «Adquisición y puesta en marcha de equipamiento para control manual en puestos fronterizos en el marco del sistema de entradas y salidas (ENTRY EXIT SYSTEM/EES)», *Plataforma del Contractación del Sector Público*, https://contrataciondelestado.es/wps/wcm/connect/f3cb2800-421f-4c30-955e-09a1909f6c67/DOC_CD2021-403985.html?MOD=AJPERES

4.

Réseaux de technologie policière

Au-delà du programme de recherche sur la sécurité, toute une série d'acteurs différents ont utilisé les fonds et les forums de l'UE pour faire avancer les plans de renforcement des contrôles d'identité biométrique mobile. En 2008, le Centre commun de recherche de l'UE a organisé une conférence qui a rassemblé quelque 70 responsables de la police et de l'immigration pour discuter de «leurs points de vue et expériences basés sur les premiers essais d'utilisation de dispositifs mobiles pour l'identification et l'authentification des personnes». L'objectif était de lancer «une discussion sur l'identification mobile qui aborderait des questions importantes telles que les meilleures pratiques en matière de processus et de procédures, les normes techniques, leur évaluation de manière harmonisée au niveau paneuropéen et l'interopérabilité entre les différentes solutions disponibles ou adoptées».[80]

Cela a conduit à la création du groupe européen d'interopérabilité de l'identification mobile (*European Mobile Identification Interoperability Group* - e-MOBidIG), dirigé par Frank Smith, un fonctionnaire de la UK Border Agency. En 2011, il comptait cinq sous-groupes et des représentants du secteur étaient régulièrement invités à ses réunions. En mars 2010, les réponses à un questionnaire diffusé parmi les membres du groupe ont montré que huit États membres de l'UE (parmi ceux qui ont répondu) utilisaient ou testaient des dispositifs d'identification mobiles, et que six d'entre eux utilisaient ces dispositifs à des fins de contrôle aux frontières.[81] Le groupe a finalement été intégré à une entité plus vaste, le Réseau européen des services technologiques des forces de l'ordre (*European Network of Law Enforcement Technology Services* - ENLETS).

ENLETS a également vu le jour en 2008, sur la base d'une idée avancée par la délégation française au groupe de travail «Coopération policière» du Conseil de l'UE, à savoir «un réseau informel de chefs de service chargés de mettre en œuvre les nouvelles technologies dans les services de police». Il a fallu un certain temps pour que le réseau prenne de l'ampleur,[82] mais en 2012, un «groupe central» avait été créé et s'était mis d'accord sur un certain nombre de domaines prioritaires, notamment diverses technologies de surveillance (reconnaissance automatique des plaques d'immatriculation, écoute discrète et drones) et les armes non létales, entre autres.[83]

En 2013, ENLETS a reçu l'approbation politique de haut niveau du Conseil «Justice et Affaires intérieures» et la Commission européenne a commencé à fournir un financement,[84] qui s'est poursuivi depuis lors.[85]

Lorsque e-MOBidIG est devenu partie intégrante d'ENLETS, il s'est transformé en un sous-groupe connu sous le nom de « groupe mobile ENLETS» . En 2017, le groupe mobile a produit un rapport qui déclarait qu'un «tournant» avait été atteint en termes de possibilités offertes à la police par les nouvelles technologies. «La technologie mobile est désormais une force perturbatrice de la réforme», indiquait le document, qui devait permettre aux agents d'avoir un accès instantané, 24 heures sur 24 et 7 jours sur 7, aux données, profils, images, vidéos et éléments biométriques de toute personne arrêtée, contrôlée ou sous surveillance.[86]

Selon le rapport, ceci se ferait principalement par le biais d'un accès mobile aux bases de données de l'UE, ce qui nécessiterait «de nouvelles règles pour le fonctionnement des systèmes nationaux et européens» - précisément le type de règles introduites par l'initiative «interopérabilité», dont les propositions ont été publiées le mois précédent le rapport ENLETS.[87] Le rapport souligne également l'importance de «contrôles d'identité approfondis en tant que première étape obligatoire de tout processus», tout en soulignant que des changements organisationnels et procéduraux majeurs et complexes seraient nécessaires pour mettre en œuvre sa vision de la «police mobile» :

> *«La mise en œuvre de solutions mobiles à grande échelle dans les services de police est une entreprise majeure... elle implique un processus de changement intégral sur la plupart des aspects de l'organisation et, en tant que telle, une priorité de niveau stratégique s'impose».*[88]

On ignore si des mesures immédiates ont été prises pour encourager le «processus de changement intégral». Cependant, quelques années plus tard, en novembre 2020, une note de la présidence allemande du Conseil adressée au groupe de travail du Conseil sur l'échange d'informations demandait un «changement de paradigme» qui introduirait :

> *«...la nécessité d'une nouvelle architecture d'information intégrée pour la sécurité intérieure, la gestion des frontières et la migration. Elle devrait consolider les capacités des technologies numériques et des informations disponibles et fournir un outil étendu et puissant aux praticiens, augmentant l'efficacité de leur travail quotidien».*

La présidence a noté que ce problème était traité par la construction et l'interconnexion de bases de données à grande échelle, nouvelles et existantes, via l'initiative d'interopérabilité. Toutefois, la présidence a également souligné que pour que l'interopérabilité ait un «effet maximal», les données saisies dans ces systèmes devaient être «de très haute qualité» et les utilisateurs des systèmes devaient y avoir «un accès rapide, sûr et complet». Cela nécessiterait :

80 «Europe's police and immigration "mobile identification" enthusiasts prepare to regroup during Irish Presidency of the EU», Statewatch news online, 28 mars 2012, https://www.statewatch.org/news/2013/january/statewatch-news-online-eu-europe-s-police-and-immigration-quot-mobile-identification-quot-enthusiasts-prepare-to-regroup-during-irish-presidency-of-the-eu/

81 Ibid.

82 Eric Töpfer, «A new player in Security Research : the European Network of Law Enforcement Technology Services (ENLETS)», 1er avril 2011, https://www.statewatch.org/statewatch-database/eu-a-new-player-in-security-research-the-european-network-of-law-enforcement-technology-services-enlets-by-eric-topfer/.

83 «EU : European police step up cooperation on technological research and development», *Statewatch*, 26 novembre 2012, https://www.statewatch.org/news/2012/november/eu-european-police-step-up-cooperation-on-technological-research-and-development/

84 «EU : New police cooperation plan includes surveillance, intelligence-gathering and remote vehicle stopping technology», *Statewatch*, 23 janvier 2014, https://www.statewatch.org/news/2014/january/eu-new-police-cooperation-plan-includes-surveillance-intelligence-gathering-and-remote-vehicle-stopping-technology/

85 «EU funding for network developing surveillance, intelligence-gathering and remote vehicle stopping tools», *Statewatch*, 15 janvier 2015, https://www.statewatch.org/news/2015/january/eu-funding-for-network-developing-surveillance-intelligence-gathering-and-remote-vehicle-stopping-tools/

86 «Total information awareness for law enforcement : 'turning point' reached, says EU police technology network», *Statewatch*, 4 juillet 2017, https://www.statewatch.org/news/2017/july/total-information-awareness-for-law-enforcement-turning-point-reached-says-eu-police-technology-network/

87 Commission européenne, «Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration)», 12 décembre 2017, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017PC0794

88 « Total information awareness for law enforcement : 'turning point' reached, says EU police technology network», *Statewatch*, 4 juillet 2017, https://www.statewatch.org/news/2017/july/total-information-awareness-for-law-enforcement-turning-point-reached-says-eu-police-technology-network/

«…un nouvel éco-système de dispositifs et de solutions pour l'acquisition de données brutes et l'accès à l'information aux fins de la sécurité intérieure, de la gestion des frontières et des migrations, ainsi que la poursuite du renforcement de la cybersécurité».[89]

L'adoption de normes et de procédures techniques communes à tous les États membres a été identifiée comme le meilleur moyen de garantir que des données de qualité suffisante soient introduites dans les systèmes, puis mises à disposition et accessibles de manière uniforme. Le groupe de travail sur l'échange d'informations a donc adopté une «feuille de route» [90] destinée à guider l'adoption de normes pour :

→ la qualité des données biométriques ;
→ qualité des données alphanumériques ;
→ des dispositifs pour l'acquisition de données biométriques brutes ; et
→ les dispositifs et solutions mobiles.

La présidence portugaise a ensuite présenté un «plan d'action pour la mise en œuvre de la feuille de route».[91] Une panoplie d'agences, de groupes de travail et d'institutions sont impliqués, sous la coordination de «eu-Lisa» [92], l'agence de l'UE pour les bases de données de la justice et des affaires intérieures. Les activités comprennent l'élaboration de propositions de normes techniques internationales pour encourager les entreprises à développer des produits conformes aux exigences de l'UE,[93] l'élaboration par les agences de l'UE de programmes de formation sur l'acquisition et l'utilisation de la biométrie, et la création d'un «catalogue de référence des dispositifs et des solutions pour l'acquisition de données et l'accès aux informations dans les systèmes centraux (SIS, VIS, EES, ECRIS-TCN, EURODAC)».

Ce catalogue informera les autorités nationales des équipements disponibles pour les agents de police, les gardes-frontières et autres personnes cherchant à saisir ou à accéder à des données dans les systèmes d'information de l'UE, et couvrira les points suivants :

→ les scanners d'images faciales fixes et portatifs ;
→ les scanners d'empreintes digitales et de paumes de mains fixes et portatifs ;
→ «autres solutions d'identification biométrique qui pourraient s'avérer pertinentes à l'avenir» ;
→ les lecteurs et scanners de documents ;
→ «les solutions mobiles pour l'accès à l'information (par exemple, les appareils de poche utilisés par les gardes-frontières et les autorités chargées de faire respecter la loi)».[94]

Frontex, Europol, l'Agence européenne pour l'asile, les autorités nationales, la DG HOME de la Commission et le Centre commun de recherche de l'UE doivent soutenir la création du catalogue en fournissant des informations à eu-Lisa. Ils sont également chargés de réaliser des enquêtes, des études et des analyses sur les «exigences commerciales et opérationnelles», sur «l'impact et les résultats des initiatives en cours concernant l'avenir des voyages» [95], et de transformer les «exigences commerciales» aux «niveaux stratégique, tactique et opérationnel en exigences fondées sur des solutions pour les nouveaux systèmes, les initiatives et les refontes [réformes juridiques]».[96]

Derrière ce jargon, ce dernier point démontre qu'il ne s'agit pas simplement d'un exercice technique visant à faciliter la mise en œuvre de mesures juridiques et politiques qui ont été convenues par les institutions de l'UE - il s'agit également de créer un moyen pour que les «exigences» des agences et institutions publiques soient prises en compte dans les nouvelles politiques et lois. À cet égard, il convient de souligner que si les «feuilles de route» et les «plans d'action» peuvent être des moyens utiles pour un large éventail d'acteurs et d'organisations de coordonner leurs activités, le fait qu'ils tendent à être tenus à l'écart du public et destinés uniquement à être discutés par un nombre limité de fonctionnaires ne laisse pas beaucoup de place au contrôle démocratique ou à la délibération.

89 Le document est disponible ici : «EU : Beefing up police databases : plans for increased input, data quality roadmap, automation», *Statewatch*, 24 novembre 2020, https://www.statewatch.org/news/2020/november/eu-beefing-up-police-databases-plans-for-increased-input-data-quality-roadmap-automation/

90 Conseil de l'UE, «Roadmap for standardisation for data quality purposes», 11 novembre 2020, pdf, disponible ici : https://www.statewatch.org/news/2020/november/eu-beefing-up-police-databases-plans-for-increased-input-data-quality-roadmap-automation/. Cette feuille de route fait suite à une précédente «Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area», 6 juin 2016, https://www.statewatch.org/media/documents/news/2016/jun/eu-council-info-exchange-interoperability-road-map-9368-rev1-6-6-16.pdf

91 Conseil de l'UE, «Action Plan for the implementation of the Roadmap for standardisation», document du Conseil 9105/21, 16 juin 2021 (non publié actuellement).

92 L'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice..

93 Le rapport note : «Comme suggéré ci-dessus, l'alignement sur les normes internationales des systèmes biométriques développés et exploités par eu-LISA, ainsi que de ceux utilisés par les autorités des États membres, sera essentiel pour garantir une qualité élevée des données biométriques» . Depuis 2021, avec les représentants de plusieurs États membres de l'UE, eu-LISA participe à l'élaboration de la famille de normes ISO [Organisation internationale de normalisation] sur la biométrie, par le biais d'une liaison avec le sous-comité de normalisation ISO/IEC/JTC1/SC37. Bien que des représentants experts d'un certain nombre d'autorités des États membres de l'UE participent déjà aux travaux de normalisation du sous-comité susmentionné, le renforcement de l'engagement des États membres de l'UE dans les travaux de normalisation contribuera à orienter le développement de normes internationales dans le domaine de la biométrie et des exigences spécifiques à bord pertinentes dans le contexte de l'UE. L'élévation des exigences de l'UE au rang de normes internationales pourrait donner un élan supplémentaire à l'industrie pour développer des technologies et des solutions répondant à ces exigences spécifiques, et donc potentiellement renforcer la concurrence sur le marché».

94 « Creation of a Reference Catalogue of Devices and Solutions for the Acquisition of Data and Access to Information in the Central Systems» , dans The eu-LISA Bits & Bytes Digital Newsletter, décembre 2020, https://eulisa.europa.eu/SiteAssets/Bits-and-Bytes/002.aspx

95 Il s'agit notamment d'une étude commandée par Frontex au début de 2021 et dont la publication est prévue cette année. Voir : «Technology Foresight on Biometrics for the Future of Travel» , 18 février 2021, https://frontex.europa.eu/media-centre/news/news-release/new-research-study-technology-foresight-on-biometrics-for-the-future-of-travel-ugObkJ

96 Conseil de l'UE, «Action Plan for the implementation of the Roadmap for standardisation», document du Conseil 9105/21, 16 juin 2021 (non publié actuellement).

En ce qui concerne l'identification et la vérification des personnes, la collecte de données biométriques, telles que les images faciales et les empreintes digitales, est censée contribuer à résoudre le problème des données incorrectes ou incomplètes : en utilisant la mesure numérisée des caractéristiques physiques, les informations peuvent être «attachées» (*fixed*) à un individu. Cependant, le fait qu'un grand nombre de personnes soient forcées d'utiliser de fausses identités pour franchir les frontières et se mettre en sécurité peut conduire à ce qu'elles se retrouvent «coincées» avec cette identité.

Depuis 2019, les enfants migrants non accompagnés en France sont obligés de faire enregistrer leurs données biométriques et autres dans un fichier centralisé pour pouvoir bénéficier d'une aide : un fait que la Commission européenne a un jour désigné comme étant le principe du «pas d'enregistrement, pas de droits» (*no registration no rights*).[97] L'objectif officiel de ce système est de «mieux garantir la protection des enfants» et de «lutter contre l'entrée et le séjour irréguliers d'étrangers en France».[98] Cependant, les enfants qui ont voyagé dans l'UE avec un faux passeport (d'adulte) ont été considérés comme s'ils étaient cette personne adulte, ce qui signifie qu'ils n'ont pas eu accès aux services et aux soins requis pour les enfants. De même, les enfants qui refusent de donner leurs empreintes digitales sont, par défaut, traités comme des adultes.[99]

Un certain nombre d'autorités régionales ont refusé de participer à un système qu'elles considéraient comme allant à l'encontre de l'intérêt supérieur des enfants.[100] L'État leur a alors coupé les vivres. En réponse, un groupe d'organisations de défense des droits humains a demandé au gouvernement de supprimer l'ensemble du système d'enregistrement biométrique des enfants, qui, selon elles, repose sur une «confusion entre la protection de l'enfance et la lutte contre l'immigration irrégulière».[101]

Ainsi, des données saisies par erreur (par exemple, des noms mal orthographiés ou d'autres détails), ainsi que des données fausses ou trompeuses (mais nécessaires pour que la personne concernée puisse atteindre la sécurité) sont toutes deux susceptibles d'avoir des effets négatifs pour les individus. C'est d'autant plus vrai en raison de la déférence officielle envers les données qui ont été formellement enregistrées dans un système ou un autre : «Selon des fonctionnaires, des avocats et des experts, les informations fournies par un système informatique bénéficient d'une grande confiance», indique un rapport de l'Agence des droits fondamentaux de l'UE.[102] Comme l'a déclaré à *Statewatch* Nicholas Chevreux, avocat spécialisé dans les questions d'asile en Allemagne : «nous pouvons seulement expliquer pourquoi l'enregistrement est erroné, pourquoi les données dans la base de données sont erronées. Mais c'est extrêmement difficile, et il est presque impossible de convaincre [quiconque] que l'ordinateur s'est trompé».

En outre, malgré l'augmentation constante de la collecte de données, les individus exercent rarement leur droit d'y accéder pour en vérifier la véracité et la légalité.[103] Avec tant d'autres problèmes à régler, il est peu probable que les personnes qui se trouvent dans le système d'asile cherchent à corriger les données détenues à leur sujet, en particulier pour des détails comme l'orthographe du nom, malgré le caractère central d'une information exacte pour une prise de décision légitime. Il y a bien sûr une tension ici : s'il existe une obligation légale générale pour les données personnelles traitées par les autorités publiques d'être exactes et à jour,[104] prendre ce présupposé comme point de départ dans l'analyse d'un projet ou d'une initiative donnée permet d'éviter les questions sur la légitimité de cette collecte de données en premier lieu.

97 Document officieux de la Commission européenne, «No registration no rights», 2015, https://www.statewatch.org/media/documents/news/2015/dec/eu-com-No-registration-no-rights.pdf.

98 «Le fichier censé mieux prendre en charge les mineurs isolés a été créé», *Le Monde*, 31 janvier 2019, https://www.lemonde.fr/societe/article/2019/01/31/un-fichier-controverse-des-mineurs-isoles-etrangers-va-voir-le-jour_5417343_3224.html

99 Maïa Courtois, «Comment le fichage biométrique renforce l'errance des mineurs isolés», *Numerama*, 8 novembre 2020, https://www.numerama.com/politique/663357-comment-le-fichage-biometrique-renforce-lerrance-des-mineurs-isoles.html

100 Maïa Courtois, «Comment le fichage biométrique renforce l'errance des mineurs isolés», *Numerama*, 8 novembre 2020, https://www.numerama.com/politique/663357-comment-le-fichage-biometrique-renforce-lerrance-des-mineurs-isoles.html

101 «L'État décide de frapper au porte-monnaie les départements qui résistent au fichage des enfants», *Gisti*, 7 juillet 2020, https://www.gisti.org/spip.php?article6438.

102 Agence des droits fondamentaux, « Fundamental rights and the interoperability of EU information systems : borders and security», mai 2017, p.33, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf

103 «La grande majorité des États membres ont informé qu'ils n'ont enregistré aucune demande d'accès depuis juillet 2016. Un État membre a informé qu'il avait enregistré 6 demandes fin 2016, 55 demandes en 2017 et 20 demandes début 2018. Plusieurs États membres ont informé qu'ils ont des enregistrements de deux demandes et un a signalé moins de 5». Voir : Eurodac SCG, «Report on the exercise of data subjects' rights in relation to Eurodac», novembre 2019, p.p.9, https://edps.europa.eu/sites/edp/files/publication/2019_11_eurodac_report_data_subjects_rights_en.pdf

104 Article 5, «Principes relatifs au traitement des données à caractère personnel», Règlement général sur la protection des données, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679 s

5.

Technologie avancée, pratiques régressives

Les technologies, politiques et lois qui sous-tendent les initiatives de l'UE en matière d'identité biométrique sont mises en œuvre dans des sociétés où prévaut le racisme et la discrimination. Il est clairement établi que le profilage racial et ethnique est endémique tant dans la police que dans la police aux frontières, tant en Europe que au-delà. Un rapport du Conseil de l'Europe de décembre 2020 décrit le profilage racial et ethnique dans le travail de la police comme «une question très préoccupante»,[105] tandis qu'une enquête de 2017 de l'Agence des droits fondamentaux de l'UE a identifié le profilage ethnique comme «faisant partie de la boîte à outils de la police».[106]

L'ajout d'une nouvelle composante technologique aux contrôles d'identité ne contribuera guère à remédier à ce problème. Bien au contraire, il est probable qu'elle l'exacerbera encore. Alors que les autorités cherchent à augmenter le nombre d'expulsions[107] et que la couleur de la peau est considérée comme un indicateur du statut migratoire d'une personne, toute tentative d'augmenter le nombre de contrôles d'identité a de graves conséquences pour les minorités ethniques, qu'elles soient européennes ou non. Bien qu'il puisse exister des garanties - par exemple, dans les lois européennes sur la protection des données ou dans la législation sur l'interopérabilité elle-même - celles-ci peuvent simplement être ignorées[108] ou insuffisantes.[109]

Profilage ethnique par la police

Une enquête réalisée en 2018 par l'Agence des droits fondamentaux de l'UE (FRA) auprès de plus de 5 800 personnes d'ascendance africaine dans 12 États membres de l'UE a montré que 24% des répondants avaient été interpellés par la police au cours des cinq années précédant l'enquête ; et 11% au cours des 12 mois précédant l'enquête.[110]

Parmi les personnes interpellées au cours des 12 derniers mois, 44% considèrent que «la dernière interpellation qu'elles ont subie était motivée par le racisme», bien que cette perception diffère largement entre les personnes vivant dans différents États [111] ainsi que entre les hommes et les femmes.[112]

Au-delà des perceptions individuelles, d'autres données démontrent la disproportionnalité raciale des contrôles de police. En Espagne, la FRA a identifié dans une enquête de 2008 que 42% des contrôles de police visaient des personnes d'origine Nord-africaine, 81% d'entre eux ayant lieu dans la rue ou dans les transports publics.[113] D'autres recherches entreprises en 2016 par la *Asociación Pro Derechos Humanos de Andalucía* et l'Université de Grenade ont révélé que les personnes africaines étaient 42 fois plus susceptibles de se voir demander une pièce d'identité que les personnes blanches, tandis que les Roms étaient 12 fois plus susceptibles, les Nord-Africains 10 fois plus susceptibles et les Latino-américains sept fois plus susceptibles. Dans tous les cas, les jeunes hommes sont les plus susceptibles d'être arrêtés.[114] Des disproportions tout aussi frappantes ont été identifiées en Catalogne[115] et en 2018, un groupe d'experts de l'ONU a décrit le profilage ethnique des personnes d'origine africaine comme étant «endémique» en Espagne.[116] Le recours à la police et à l'armée pour faire respecter l'état d'urgence mis en place par le gouvernement en mars 2020 en réponse à la propagation du coronavirus a offert une démonstration claire de cette tendance, avec au moins 30 cas de profilage racial signalés par des organisations antiracistes au cours des trois premières semaines des mesures d'urgence à Madrid.[117]

Il y a eu des contestations de ces pratiques mais les résultats en ont été mitigés. En 2001, dans l'affaire *Rosalind Williams*, la Cour constitutionnelle du pays a sanctionné l'hypothèse selon laquelle les ressortissants espagnols ne

105 Conseil de l'Europe, Comité pour l'égalité et la non-discrimination. «Le profilage ethnique en Europe : une question très préoccupante» , 14 décembre 2020, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28889&lang=en

106 FRA, «Second European Union Minorities and Discrimination Survey. Main results», 2017, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-eu-midis-ii-main-results_en.pdf

107 *Statewatch*, «Deportation Union : Rights, accountability and the EU's push to increase forced removals» 19 août 2020, https://www.statewatch.org/deportation-union-rights-accountability-and-the-eu-s-push-to-increase-forced-removals/

108 *Human Rights Watch* note à propos du programme d'identification biométrique mobile mis en place par la police grecque : «Dans sa forme actuelle, le nouveau programme ne serait pas conforme au droit grec et européen». L'autorité grecque de protection des données a ouvert une enquête. Voir : «Grèce : New Biometrics Policing Program Undermines Rights», *Human Rights Watch*, 18 janvier 2022, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

109 Un précédent rapport de *Statewatch* sur l'initiative d'interopérabilité soulignait que «si la législation contient des garanties anti-discrimination, elles sont extrêmement faibles». Voir : Data Protection, Immigration Enforcement and Fundamental Rights : What the EU's Regulations on Interoperability Mean for People with Irregular Status, *Statewatch*/*PICUM*, 18 novembre 2019, https://www.statewatch.org/publications/reports-and-books/data-protection-immigration-enforcement-and-fundamental-rights-what-the-eu-s-regulations-on-interoperability-mean-for-people-with-irregular-status/

110 Agence des droits fondamentaux, « Être noir dans l'UE» , 2018, p.30, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-being-black-in-the-eu-summary_fr.pdf.

111 Par exemple : «en Autriche, le taux auquel la dernière interpellation policière a été perçue comme un profilage ethnique est presque huit fois plus élevé que celui de la Finlande (31% contre 4%), si l'on considère la période de 12 mois précédant l'enquête».

112 «Les hommes ont trois fois plus de probabilité d'être arrêtés que les femmes (22% contre 7%) et quatre fois plus de probabilité de percevoir le contrôle le plus récent comme étant un profilage racial (hommes : 17%, femmes : 4%)»

113 Agence des droits fondamentaux, «Police Stops and Minorities», 2010, https://fra.europa.eu/fraWebsite/attachments/EU-MIDIS-police.pdf

114 Identificaciones basadas en perfil étnico en Granada», *APDHA*/*Instituto de la paz y los conflictos*, 2016, https://www.pareudepararme.org/uploads/2016_Granada_APDHA_identificaciones-etnicas.pdf

115 SOS Racisme Catalunya I plataforma d'entitats Pareu de Parar-me, «L'aparença no es motiu ; indetificacions policials per perfil ètnica Catalunya. Informe 2018», 2018, https://www.pareudepararme.org/informe-ca/ ; «Ethnic profiling in Catalonia : for every police identity check on a Spanish national, there are seven checks on foreigners», *Statewatch*, 10 avril 2019, https://www.statewatch.org/news/2019/april/spain-ethnic-profiling-in-catalonia-for-every-police-identity-check-on-a-spanish-national-there-are-seven-checks-on-foreigners

116 « Statement to the media by the United Nations Working Group of Experts on People of African Descent, on the conclusion of its official visit to Spain, 19-26 February 2018», 26 février 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22705

117 Yassine Boubout et Sara Ignat, 'Who protects us from the Police ? Structural Racism in Law Enforcement in the European Union «, *Equinox Initiative for Racial Justice*, juin 2021, https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf ; « Policing the pandemic. Human rights violations in the enforcement of Covid 19 measures in Europe», *Amnesty International*, 2020, https://www.amnesty.eu/wp-content/uploads/2020/06/Report-Policing-the-pandemic-FINAL-.pdf ; «Crisis sanitaria COVID-19 : Racismo y xenophobia durante el estado de alarma en España, *Rights International Spain*, 2020, https://rightsinternationalspain.org/uploads/publicacion/d0b782ac0452e-9052241b17a646df19ad4edf12c.pdf

pouvaient être que blancs, en décidant que l'utilisation de caractéristiques ethniques comme base des contrôles de police n'était pas discriminatoire dans le contexte du contrôle de l'immigration. Mme Williams a fait l'objet d'un contrôle d'identité au motif que sa couleur de peau signifiait qu'elle pouvait être une «immigrante illégale». Après avoir essuyé de multiples échecs devant les tribunaux espagnols, elle a porté l'affaire devant le Comité des droits humains des Nations unies, qui a «conclu que la loi devait être modifiée, que le gouvernement espagnol devait présenter des excuses publiques à Rosalind Williams» et que l'Espagne devait «prendre toutes les mesures nécessaires pour empêcher ses fonctionnaires de commettre des actes comme dans le cas présent».[118]

Néanmoins, la décision de la Cour constitutionnelle dans l'affaire Williams «n'a pas encore été annulée», a noté *l'Open Society Justice Initiative* en 2016.[119] Une affaire pendante devant la Cour européenne des droits humains[120]concernant un ressortissant pakistanais et résident espagnol, Zeshan Muhammad, pourrait y remédier. Muhammad a été arrêté avec un ami par la police à Barcelone en 2013, soupçonné d'être en Espagne de manière irrégulière.[121] L'agent en question a utilisé un «langage à connotation raciale» pour expliquer que la couleur de la peau de Muhammad était la raison de l'interpellation.[122] Muhammad a porté plainte, estimant qu'un tel profilage ethnique violait la constitution espagnole et les traités internationaux. L'affaire a été rejetée par la Haute Cour et la Cour constitutionnelle espagnoles et est actuellement en attente d'une audience à Strasbourg.

L'affaire Williams a été suivie de quelques changements dans les pratiques. La police nationale espagnole s'est engagée à définir et à interdire le profilage ethnique lors des contrôles d'identité, notamment en prenant des mesures pour enregistrer tous les cas et consigner l'origine ethnique perçue des personnes appréhendées.[123] D'autres initiatives ont également cherché à améliorer la situation. Un projet pilote entrepris par la Plate-forme pour la gestion policière de la diversité (*Plataforma por la Gestión policial de la Diversidad*) a réuni des associations de police et des organisations de lutte contre la discrimination afin de promouvoir les Bonnes pratiques dans la police dans le domaine de la non-discrimination.[124] Dans le cadre de ce projet pilote, des «formulaires de contrôle (*stop forms*)» ont été adoptés. Les enregistrements des contrôles effectués dans cinq départements de police espagnols ont démontré que le fait de devoir enregistrer les interpellations et les fouilles avait entrainé une diminution des contrôles discriminatoires.[125] Toutefois, l'organisme national de la police n'a pas vraiment suivi le mouvement.[126] Dans les localités où le modèle a été introduit, le manque de retour d'information de la part des hauts fonctionnaires a contribué à réduire les taux d'amélioration, tandis qu'à Gérone, les policiers ont même augmenté les interpellations de personnes non blanches par frustration face à la nouvelle politique.[127]

En France, comme en Espagne, il n'existe pas de collecte officielle de données sur l'origine ethnique des personnes contrôlées lors des contrôles d'identité. Une étude de *l'Open Society Initiative* menée en 2009 a révélé que les personnes étaient six fois plus susceptibles d'être contrôlées si elles étaient noires, et presque huit fois plus si elles semblaient être d'origine arabe.[128] Un ancien médiateur français a déclaré que «par rapport à la population générale et toutes choses égales par ailleurs, les jeunes hommes en France, qui sont perçus comme arabes/maghrébins ou noirs, ont 20 fois plus de chances d'être soumis à des contrôles d'identité que les autres».[129] Le Haut-Commissaire des Nations unies aux droits humains a épinglé la France en ce qui concerne les contrôles de police discriminatoires en juin 2021.[130]

Le mois suivant, six organisations de la société civile ont déposé un recours collectif exigeant des réformes structurelles et des mesures pour mettre fin à la discrimination dans les pratiques policières, notamment une réglementation plus stricte, une meilleure formation de la police et l'élaboration de rapports de suivi concernant les contrôles d'identité et de leur impact.[131] Auparavant, en 2016, la Cour de cassation a reconnu la responsabilité de l'État dans une affaire de contrôles d'identité discriminatoires de trois personnes, traitement qui s'apparentait à une «faute grave».[132] La Cour a souligné le fait que les contrôles ont été effectués pendant une heure et demie, qu'ils ciblaient des membres de «minorités visibles» et que l'État n'a pas réussi à démontrer qu'il existait des raisons objectives pour justifier ces contrôles.

En Italie, des études ethnographiques indiquent des problèmes similaires. L'universitaire Martina Tazzioli a entrepris des recherches approfondies sur le terrain dans la région frontalière entre l'Italie et la France - une frontière intérieure entre deux États membres de l'UE où l'on cherche actuellement à renforcer les contrôles d'identité (cet aspect est expliqué plus loin). Lorsque les soulèvements du printemps arabe ont entraîné un pic des départs irréguliers de personnes à travers la Méditerranée, Tazzioli a constaté que :

118 Williams c. Espagne, *Open Society Justice Initiative*, sans date, https://www.justiceinitiative.org/litigation/williams-v-spain

119 «Police Ethnic Profiling Challenge Goes Before Spain's Constitutional Court», *Open Society Foundations*, 29 juin 2016, https://www.opensocietyfoundations.org/newsroom/police-ethnic-profiling-challenge-goes-spains-constitutional-court

120 Muhammad c. Espagne», *Cour européenne des droits humains*, https://hudoc.echr.coe.int/eng?i=001-179961

121 « Police Ethnic Profiling Challenge Goes Before Spain's Constitutional Court», *Open Society Foundations*, 29 juin 2016, https://www.opensocietyfoundations.org/newsroom/police-ethnic-profiling-challenge-goes-spains-constitutional-court

122 Muhammad c. Espagne, *Cour européenne des droits humains*, https://hudoc.echr.coe.int/eng?i=001-17996

123 Ministerio del Interior, Circular núm. 2/2012 de la Dirección General de la Policía sobre identificación de ciudadanos, 16 mai 2012, https://www.sup.es/sites/default/files/pdf/circular_identificaciones.pdf

124 «Chapter 7 : Engaging with the police» dans Open Society Initiative for Europe, «Challenging Ethnic Profiling in Europe : A guide for campaigners and organisers', 2021, https://www.justiceinitiative.org/uploads/78315b73-df6d-427a-a230-6cf4c4a72876/challenging-ethnic-profiling-in-europe-april-2021.pdf

125 Ibid.

126 Ibid.

127 Ibid.

128 Open Society Justice Initiative, «Profiling Minorities : A Study of Stop-and-Search Practices in Paris», 2009, https://www.justiceinitiative.org/publications/profiling-minorities-study-stop-and-search-practices-paris

129 Voir le point 40 dans «Le profilage ethnique en Europe : une question très préoccupante», 14 décembre 2020, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28889&lang=fr

130 Haut-Commissaire des Nations unies aux droits humains, « Promotion et protection des droits de l'homme et des libertés fondamentales des Africains et des personnes d'ascendance africaine face au recours excessif à la force et aux autres violations des droits de l'homme dont se rendent coupables des membres des forces de l'ordre», 1er juin 2021, https://undocs.org/A/HRC/47/53.

131 « France : Class action action against ethnic profiling filed over systemic racial discrimination», *Amnesty International*, 22 juillet 2021, https://www.amnesty.org/en/latest/news/2021/07/france-class-action-lawsuit-against-ethnic-profiling-filed-over-systemic-racial-discrimination-2/

132 «Jurisprudence sur le profilage ethnique dans les contrôles de police», *GISTI*, http://www.gisti.org/spip.php?article5872#vi ; «France : Mettre fin aux discriminations policières systémiques. Civil Society Organizations File Class Action Challenging Ethnic Profiling», *Human Rights Watch*, 27 janvier 2021 https://www.hrw.org/news/2021/01/27/france-end-systemic-police-discrimination

> *«Vintimille [ville située à la frontière entre l'Italie et la France] s'est révélée être une frontière intermittente racialisée : en 2011 comme en 2015, Schengen n'était en effet suspendu que pour les ressortissants de pays tiers et des contrôles d'identité étaient donc effectués par les autorités françaises dans le train reliant Milan à Marseille, essentiellement sur la base de la couleur de peau des personnes».*[133]

Une situation similaire a été documentée à la frontière franco-espagnole. Iker Barbero a analysé la situation à Irun/Hendaye, concluant que la frontière interne censée avoir été supprimée par l'accord de Schengen reste très présente, et que des contrôles discriminatoires fondés sur la suspicion d'un statut d'immigré clandestin y ont fréquemment lieu.[134]

Si, dans certains cas, ces pratiques peuvent être le fait d'agents de police ayant des préjugés individuels, de nombreux éléments indiquent que le problème vient également d'en haut.[135] L'organisation juridique espagnole *Iridia* a rapporté qu'en réponse à de fausses informations médiatiques selon lesquelles des demandeurs d'asile étaient transférés en masse depuis les îles Canaries vers la péninsule espagnole, le ministère de l'Intérieur a autorisé l'introduction de contrôles d'identité dans les ports et les aéroports sur la base de critères ethnico-raciaux,[136] en violation des dispositions juridiques nationales qui autorisent la liberté de circulation sur l'ensemble du territoire espagnol pour les demandeurs d'asile.[137] On estime que 5 000 personnes ont été empêchées de quitter les îles depuis décembre 2020.[138]

En Italie, les contrôles d'identité ont été renforcés à partir de 2015 dans le cadre de la traque des migrants en situation irrégulière. En janvier 2017, une circulaire du ministère de l'Intérieur envoyée à tous les quartiers généraux de la police indiquait que dans le cadre de la coopération avec l'ambassade du Nigéria à Rome, 95 places dans les centres de détention pour immigrés avaient été réservées pour faciliter l'expulsion des citoyens nigérians. Les directions générales de la police étaient donc «invitées à effectuer des interpellations ciblées dans le but de retrouver les citoyens nigérians en situation irrégulière sur le territoire national».[139] Des activités similaires ont été signalées depuis longtemps en Espagne dans le but de remplir les vols d'expulsion.[140] En France, l'état d'urgence en vigueur depuis plusieurs années (instauré à la suite d'attaques terroristes en 2015) a permis de justifier une augmentation des contrôles d'identité aux frontières et ailleurs, malgré les critiques selon lesquelles la base juridique invoquée par le gouvernement ne justifie pas suffisamment cette mesure.[141]

Interopérabilité pour les contrôles d'identité

Malgré ces problèmes de longue date et bien documentés concernant les contrôles d'identité par la police, l'UE est sur le point de fournir de nouveaux moyens techniques et juridiques pour augmenter la fréquence de ces contrôles. Comme indiqué dans la section L'identification biométrique : une priorité européennel'un des principaux objectifs du projet d'interopérabilité est d'établir une vaste réserve centralisée de données d'identité, via la construction du référentiel commun d'identité, afin de «faciliter l'identification fiable, par les agents habilités, des ressortissants de pays tiers qui entrent ou se trouvent déjà sur le territoire de l'espace Schengen»[142].

Alors que le CIR fournira l'ossature technique, la volonté d'intensifier les contrôles d'identité est renforcée par des initiatives juridiques et politiques. En mai 2017, la Commission européenne a publié une «recommandation sur les contrôles de police proportionnés».[143] Ce document indique qu'en raison du terrorisme, de la criminalité transfrontalière et de la migration irrégulière :

> *«...l'intensification des contrôles de police sur l'ensemble du territoire des États membres, y compris dans les zones frontalières, et la réalisation de contrôles de police le long des principaux axes de transport tels que les autoroutes et les chemins de fer, peuvent être considérées comme nécessaires et justifiées».*

La possibilité de renforcer la surveillance et les contrôles aux frontières intérieures de l'espace Schengen est désormais susceptible d'être inscrite dans la loi, en vertu de propositions publiées en décembre 2021.[144] Celles-ci permettraient d'augmenter le nombre de patrouilles aux frontières intérieures de l'UE afin d'empêcher les «mouvements secondaires», c'est-à-dire les déplacements non autorisés d'individus, notamment de demandeurs d'asile et de réfugiés, d'un État membre à l'autre. La Commission a reconnu que les nouvelles mesures pourraient «augmenter le risque» de «profilage racial et de sélection

133 Martina Tazzioli, «Governing migrant mobility through mobility : Containment and dispersal at the internal frontiers of Europe», *Environment and Planning C : Politics and Space*, 38(1), 10 avril 2019, https://journals.sagepub.com/doi/10.1177/2399654419839065

134 Iker Barbero González, « La readmisión de extranjeros en situación irregular entre Estados miembros : consecuencias empírico-jurídicas de la gestión policial de las fronteras internas», *Cuadernos Electrónicos de Filosofía del Derecho*, 2017, https://ojs.uv.es/index.php/CEFD/article/view/10640

135 Le «racisme institutionnel» a été défini par le rapport Macpherson sur le meurtre de Stephen Lawrence comme : «L'échec collectif d'une organisation à fournir un service approprié et professionnel aux personnes en raison de leur couleur, de leur culture ou de leur origine ethnique. Il peut être vu ou détecté dans des processus, des attitudes et des comportements qui équivalent à une discrimination par le biais de préjugés involontaires, de l'ignorance, de l'irréflexion et de stéréotypes raciaux». Voir : The Stephen Lawrence Inquiry, février 1999, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/277111/4262.pdf

136 «Vulneración de derechos humanos en la Frontera Sur : Canarias y Melilla», *Irídia*, pp.57-9, https://iridia.cat/es/publicaciones/vulneracions-de-drets-humans-a-la-frontera-sud-canaries-i-melilla/

137 Defensor del pueblo, «El defenso reclama que se agilicen los traslados de personas migrantes a la peninsula», 3 mars 2021, https://www.defensordelpueblo.es/noticias/migracion-en-canarias/

138 Vulneración de derechos humanos en la Frontera Sur : Canarias y Melilla», *Irídia*, https://iridia.cat/es/publicaciones/vulneracions-de-drets-humans-a-la-frontera-sud-canaries-i-melilla ; «Informe 2020 Frontera Sur», *Servicio Jesuita a Migrantes*, 18 décembre 2020, https://sjme.org/docs/informe-2020-frontera-sur ; Gabriela Sánchez, «El Gobierno ahora sí impide la salida de migrantes de Canarias por su cuenta : «Todo está cerrado», *El Diario*, 19 décembre 2020, https://www.eldiario.es/desalambre/gobierno-ahora-si-impide-salida-migrantes-canarias-cuenta-cerrado_1_6517256.html

139 «Italy : Police instructed to target Nigerians», *Statewatch*, 2 janvier 2017, https://www.statewatch.org/news/2017/january/italy-police-instructed-to-target-nigerians/

140 «Vulneraciones de derechos en la frontera sur : Gran Canaria y Melilla», *Irídia*, janvier 2021, https://iridia.cat/wp-content/uploads/2021/01/INFORME-DDHH-FRONTERA-SUR-2021.pdf

141 Le Gisti a noté dans son examen de la jurisprudence que la simple référence au système d'alerte de sécurité «Vigipirate» ne suffit pas à justifier les contrôles d'identité, qui sont régis par l'article 78-2 du code de procédure pénale.

142 Commission européenne, «Frequently asked questions - Interoperability of EU information systems for security, border and migration management», 12 décembre 2017, https://ec.europa.eu/commission/presscorner/detail/de/MEMO_17_5241

143 Commission européenne, «RECOMMANDATION DE LA COMMISSION (UE) 2017/820 du 12 mai 2017 relative aux contrôles de police proportionnés et à la coopération policière dans l'espace Schengen», https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32017H0820

144 «EU : Asylum and borders proposals : the only attack taking place is the attack on peoples' rights», *Statewatch*, 16 décembre 2021, https://www.statewatch.org/news/2021/december/eu-asylum-and-borders-proposals-the-only-attack-taking-place-is-the-attack-on-peoples-rights/

discriminatoire des personnes contrôlées dans les zones frontalières»[145], mais n'a proposé aucune garantie spécifique contre cette possibilité, en dehors de celles qui existent déjà (par exemple, dans la Charte des droits fondamentaux de l'UE).Une recherche menée au Royaume-Uni par le Racial Justice Network, Yorkshire Resists et l'Université Queen Mary a montré un «biais racial systématique» dans l'utilisation des scanners mobiles d'empreintes digitales pour les contrôles d'identité de la police. La recherche, basée sur des données recueillies auprès des forces de police britanniques couvrant la période de mars 2019 à juin 2020, a révélé que :

> *«Sur 10 000 personnes contrôlées et scannées, pour chaque Blanc Nord-européen, 48 personnes arabes sont scannées en moyenne sur l'ensemble des juridictions policières. 14 résidents noirs sont scannés pour chaque Blanc Nord-européen, 14 Asiatiques, près de 4 Chinois ou 2 Asiatiques du Sud-Est pour chaque Blanc Nord-européen».[146]*

Les groupes ont recommandé que l'utilisation des scanners mobiles d'empreintes digitales «doit cesser immédiatement jusqu'à ce que des évaluations rigoureuses d'impact sur l'égalité aient été réalisées», et que leur utilisation devrait être étroitement surveillée s'ils sont réintroduits. Plus fondamentalement, le rapport demande aux forces de police et au ministère de l'Intérieur de s'attaquer au racisme institutionnel, de mettre en place un «pare-feu» entre les services de police et d'immigration et de mettre fin aux politiques britanniques «d'environnement hostile», que les autorités cherchent actuellement à numériser plus en avant.[147]

Les autorités grecques cherchent à mettre en œuvre un programme similaire. Grâce à un financement de l'UE, la police est en train d'acquérir des dispositifs portables de reconnaissance faciale, d'empreintes digitales et de plaques d'immatriculation de véhicules qui permettront aux agents de procéder à des vérifications instantanées par rapport aux «données déjà stockées dans 20 bases de données détenues par des autorités nationales et internationales».[148] Suite à une plainte de l'organisation de défense des droits humains *Homo Digitalis*, l'autorité de protection des données a lancé une enquête sur la légalité du programme, mais celle-ci n'est pas encore terminée. Le programme est explicitement conçu pour augmenter le nombre de contrôles d'identité, et *Human Rights Watch* a souligné que l'utilisation des technologies biométriques dans ce contexte «pourrait exacerber... les tactiques policières abusives, qui constituent des formes raciales et autres de profilage et de harcèlement».[149]

La discrimination injustifiée est interdite tant dans l'UE que par le Conseil de l'Europe, en vertu de la Charte des droits fondamentaux de l'UE et de la Convention européenne des droits humains. Néanmoins, il est évident que la réalité diverge de manière significative de ce qui est proclamé sur le papier. Malgré l'obligation faite aux autorités de procéder à des évaluations d'impact sur la protection des données et sur l'égalité, la volonté d'introduire ces technologies dans la rue risque d'exacerber les problèmes existants en matière de profilage racial et ethnique, appelant de nouvelles réponses de la part des groupes communautaires, des organisations de la société civile et de tous ceux qui aspirent à une société plus juste.

145 Commission européenne, «Rapport d'analyse d'impact accompagnant la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/399 établissant un code de l'Union relatif au régime de franchissement des frontières par les personnes», 14 décembre 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52021SC0462&from=EN

146 «STOP THE SCAN : Police use of mobile fingerprinting technology for immigration enforcement», *Racial Justice Network*, 6 mars 2021, https://racialjusticenetwork.co.uk/2021/06/03/police-scanning-report/

147 «Briefing : Resisting the Digital Hostile Environment», *JCWI, Foxglove and Liberty*, août 2021, https://www.jcwi.org.uk/briefing-resisting-the-digital-hostile-environment

148 «Grèce : New Biometrics Policing Program Undermines Rights», *Human Rights Watch*, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights

149 Ibid.

Surveillance biométrique de masse en Italie : en attente, pour le moment

La collecte et la centralisation croissantes des données biométriques ont été principalement critiquées pour le potentiel qu'elles offrent pour l'introduction d'une surveillance de masse, en particulier par l'utilisation de la technologie de reconnaissance faciale. Les autorités italiennes ont cherché avec enthousiasme à adopter de tels systèmes. Le système SARI (*Sistema Automatico Riconoscimento Immagini*) a été acquis par la *Direzione Centrale Anticrimine* de la police en 2017 grâce à l'argent du Fonds pour la sécurité intérieure de l'UE.[150]

SARI Enterprise serait utilisé pour vérifier l'authenticité des photos de documents et effectuer des contrôles automatiques en rapprochant les images faciales des images du système automatisé d'identification des empreintes digitales du pays, qui stocke également des photos. Il a été autorisé par le médiateur en juillet 2018 pour accélérer les procédures déjà entreprises à l'aide de moyens moins efficaces (vérification de détails comme la couleur des yeux ou les tatouages) pour identifier les personnes recherchées.

La même année, les plans visant à utiliser *SARI Real-Time comme*« système tactique pour surveiller les opérations de débarquement et les différents types d'activités illégales connexes, en les filmant et en identifiant les personnes impliquées» ont été bloqués.[151] Un appel d'offres de 2017 mentionnait le «soutien aux opérations de contrôle territorial lors d'événements et/ou de manifestations»,[152] indiquant clairement que ces technologies peuvent être utilisées non seulement pour cibler les non-citoyens et les minorités racisées, mais aussi les manifestants et les dissidents.

Le système italien devait s'appuyer sur un réseau de caméras vidéo pour effectuer une comparaison en temps réel avec une liste de surveillance contenant jusqu'à 10 000 images faciales, des alertes étant envoyées aux policiers en cas de correspondance. Le médiateur chargé de la protection de la vie privée n'a pas autorisé le déploiement de *SARI Real-Time* et a estimé, en 2021, que le système ne disposait pas d'une base juridique pour le traitement automatique des images faciales et qu'il était prévu comme une forme de surveillance de masse sans discernement.[153] Le médiateur s'est appuyé sur les directives du Conseil de l'Europe pour souligner le caractère sensible de cette question, notant que le déploiement de *SARI Real-Time* équivaudrait à un traitement automatisé des données à grande échelle susceptible d'affecter les participants à des manifestations sociales et politiques qui ne font pas l'objet de «l'attention» de la police.

Le cas de *SARI Real Time* a été mis en avant par les militants qui demandent l'interdiction de la surveillance biométrique de masse dans l'UE. L'étape actuelle de cette lutte est la proposition de loi sur l'intelligence artificielle, qui, dans sa forme actuelle, interdit en principe «l'identification biométrique en temps réel» dans les espaces publics, mais qui, dans la pratique, prévoit de multiples échappatoires permettant aux autorités chargées de l'application des lois de néanmoins déployer de tels systèmes.

La campagne *Reclaim Your Face* demande une interdiction totale, afin d'empêcher le suivi, la catégorisation et la surveillance injustifiés des individus. La campagne avertit que cette forme de surveillance «menace les droits et libertés de chacun à participer à la vie publique et politique». Cependant, il faut noter qu'étant donné la quantité de données biométriques stockées par les États de l'UE sur les ressortissants étrangers, il est probable que cela affecte de manière disproportionnée les non-citoyens. Par exemple, dans le cas de *SARI Real Time*, la base de données sur laquelle repose le système contient des données sur deux millions de citoyens italiens et sept millions d'étrangers.[154]

150 Riccardo Coluccini, «Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale», *Investigative Reporting Project Italy*, 13 janvier 2021, https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale

151 «Italy : Interior ministry's facial recognition system is unlawful», *Statewatch*, 21 avril 2021, https://www.statewatch.org/news/2021/april/italy-interior-ministry-s-facial-recognition-system-is-unlawful ; Garante per la Protezione dei Dati Personali, « Riconoscimento facciale : Sari Real Time non è conforme alla normativa sulla privacy «, 16 avril 2021, https://www.statewatch.org/media/2311/it-garante-privacy-sari-real-time-decision-4-21.pdf

152 Riccardo Coluccini, «Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale», *Investigative Reporting Project Italy*, 13 janvier 2021, https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale

153 Garante per la Protezione dei Dati Personali, «Riconoscimento facciale : Sari Real Time non è conforme alla normativa sulla privacy», 16 avril 2021, https://www.statewatch.org/media/2311/it-garante-privacy-sari-real-time-decision-4-21.pdf

154 Riccardo Coluccini et Laura Carrer, «Tecnologie per il controllo delle frontiere in Italia», décembre 2021, p.28, https://www.documentcloud.org/documents/21128523-tecnologie-per-il-controllo-delle-frontiere-in-italia-identificazione-riconoscimento-facciale-e-finanziamenti-europei.

6. Conclusion

L'enregistrement biométrique de tous les ressortissants étrangers présents dans l'UE est un objectif politique de longue date de l'UE, et cet objectif est en passe d'être atteint dans un futur de plus en plus proche. Beaucoup diront que cela ne pose aucun problème, à condition que les garanties nécessaires en matière de protection de la vie privée et des données soient appliquées et respectées, mais un tel point de vue ignore deux problèmes. Premièrement, ces systèmes sont conçus pour faciliter l'exclusion de certaines catégories de personnes du territoire de l'UE et de la participation à la société, ce qui soulève la nécessité de remettre en question leurs prémisses ainsi que les lois et les politiques qui les sous-tendent. Deuxièmement, comme toute autre technologie, ces systèmes sont introduits dans un contexte social particulier qui façonnera la manière dont ils sont utilisés.

Comme l'a fait valoir le présent rapport, l'introduction de nouvelles technologies visant à augmenter le nombre de contrôles d'identité effectués par la police et les services d'immigration risque de soumettre les citoyens et les non-ressortissants issus de minorités ethniques à un nombre croissant d'intrusions injustifiées dans leurs activités quotidiennes, étant donné le traitement de la couleur de la peau comme indicateur du statut migratoire. En particulier, l'existence d'une énorme base de données contenant uniquement des informations sur les ressortissants étrangers et les instructions politiques explicites visant à intensifier les contrôles d'identité signifient que l'introduction du référentiel commun d'identité et de la technologie biométrique mobile nécessaire pour y accéder est susceptible d'exacerber les pratiques policières racistes et le profilage ethnique qui existent déjà dans l'UE.

Le nombre croissant d'initiatives visant à établir des liens entre les campagnes antiracistes, les organisations de défense des droits des migrants, les défenseurs de la vie privée et de la protection des données et les spécialistes des technologies jouera un rôle important dans la remise en question de ces évolutions dans les années à venir.155 La préoccupation sociale plus large concernant les questions de racisme et de non-discrimination raciale qui a été propulsée sur le devant de la scène par l'éruption mondiale de manifestations antiracistes en réponse au meurtre de George Floyd par un policier aux États-Unis en juin 2020, ainsi que la fascination sociétale plus large pour les nouvelles technologies, peuvent fournir un terrain fertile pour l'expansion de ces initiatives. Dans le même temps, il est essentiel que l'accent mis sur la technologie elle-même ne détourne pas l'attention des structures qui la sous-tendent : les nouvelles technologies peuvent accroître la capacité de nuire, mais ne sont pas nécessairement la force motrice sous-jacente.

Il faut reconnaître que le climat politique général de xénophobie et de nationalisme n'est pas particulièrement favorable à ces efforts. Les tentatives visant à empêcher l'utilisation des nouvelles technologies d'ancrer les pratiques racistes et discriminatoires devront être menées sur plusieurs fronts : les campagnes «Connaissez vos droits» et l'organisation communautaire ; les plaintes administratives et juridiques visant à faire respecter les droits à la vie privée et à la protection des données ; les demandes de financement et de ressources adéquates pour les autorités de protection des données chargées de superviser le travail de la police et des autorités chargées de l'immigration, et pour les «pare-feu» entre la police et les services publics ; la recherche critique et le journalisme d'investigation pour étayer les campagnes et les plaintes ; les appels à ne pas utiliser les fonds publics dans des recherches susceptibles de contribuer à ancrer la discrimination ; et les efforts visant à garantir la transparence dans la législation, l'élaboration des politiques et leur application. Tous ces éléments sont essentiels pour garantir que les autorités de l'État soient tenues politiquement et publiquement responsables ainsi que pour développer des alternatives plus équitables et plus justes.

155 Par exemple : le travail de *Decolonising Digital Rights* et du Digital Freedom Fund (https://digitalfreedomfund.org/decolonising/) ; le *Migration Technology Monitor* (https://www.migrationtechmonitor.com) ; European Digital Rights (https://edri.org) ; le travail au Royaume-Uni sur «Resisting the Digital Hostile Environment», https://www.jcwi.org.uk/briefing-resisting-the-digital-hostile-environment ; le travail du *European Network on Racism* sur la police guidée par les données (https://www.enar-eu.org/Data-driven-policing-is-leading-to-racial-profiling) ; et d'innombrables autres campagnes, projets, initiatives et mouvements en Europe et au-delà.

Auteurs
Chris Jones, Jane Kilpatrick, Yasha Maccanico

Remerciements
Les auteurs souhaitent remercier toutes les personnes qui ont donné de leur temps pour être interviewées dans le cadre des recherches effectuées pour ce rapport, ainsi que toutes les personnes qui ont participé aux ateliers organisés par *Statewatch* sur la question des technologies d'identification biométrique et du racisme et de la discrimination en octobre 2021.

Méthodologie
Ce rapport est basé sur des recherches documentaires dans des sources ouvertes et fermées, des entretiens individuels et les idées générées lors des ateliers mentionnés ci-dessus. Il a été produit dans le cadre du projet «Protecting migrant communities by future-proofing the immigration data system» (*Protéger les communautés de migrants en pérennisant le système de données sur l'immigration*), soutenu par *Privacy International*.

À propos de Statewatch
Statewatch produit et promeut la recherche critique, l'analyse politique et le journalisme d'investigation pour alimenter les débats, les mouvements et les campagnes sur les libertés civiles, les droits humains et les normes démocratiques. Nous avons débuté en 1991 et sommes basés à Londres. Notre site web : statewatch.org

Publié par Statewatch, février 2022

Soutenez notre travail en faisant un don :
visitez statewatch.org/donate ou scannez le code QR ci-dessous.

Inscrivez-vous à notre liste de diffusion:
https://www.statewatch.org/about/mailing-list/

Code identifiant d'organisme caritatif enregistré au Royaume-Uni : 1154784. Code identifiant de la société britannique : 08480724. Nom de la société enregistrée : The Libertarian Research & Education Trust. Siège social : c/o MDR, 88 Fleet Street, Londres EC4Y 1DH, Royaume-Uni.