

LA PROJECTION EXTERNE DES FRONTIÈRES INTELLIGENTES DE L'UNION EUROPÉENNE: DONNÉES BIOMÉTRIQUES, COOPÉRATION UE-MAROC ET GARANTIES FONDAMENTALES

HANEN MEDROMI¹
hanenmedromi99@gmail.com

Cómo citar/Citation

Medromi, Hanen (2026).

La projection externe des frontières intelligentes de l'Union européenne: données biométriques, coopération UE-Maroc et garanties fondamentales.

Revista de Derecho Comunitario Europeo, 84, 183-230.

doi: <https://doi.org/10.18042/cepc/rdce.84.06>

Résumé

Cet article analyse la projection externe des frontières intelligentes de l'Union européenne à travers la coopération migratoire avec le Maroc. Il part du constat que le contrôle frontalier européen ne se limite plus à la vérification documentaire au point de passage, mais tend à s'organiser autour d'un régime d'identification numérique fondé sur les systèmes d'information à grande échelle, l'interopérabilité et les données biométriques. L'étude ne présume ni l'existence d'un accès direct des autorités marocaines aux bases européennes, ni celle d'un transfert généralisé de données biométriques. Elle propose plutôt une typologie juridique des formes intermédiaires de circulation informationnelle: transfert direct, accès médié, communication ponctuelle, assistance technique à l'identification et externalisation fonctionnelle du contrôle. Cette approche permet d'évaluer, mécanisme par mécanisme, les exigences découlant de la Charte des droits fondamentaux, du droit européen de la protection des données et des principes de légalité, de finalité, de nécessité, de proportionnalité, de supervision indépendante et de recours effectif. Le cas UE-Maroc montre ainsi que la coopération migratoire ne peut être juridiquement admise que si ses effets informationnels demeurent identifiables, limités, traçables et effectivement contrôlables.

¹ Doctorant chercheur à l'Université Internationale de Rabat (UIR), rattaché au Center for Global Studies (CGS), Programme doctoral en droit, Sala Al Jadida, Maroc; ORCID: <https://orcid.org/0009-0001-0630-7818>.

Mots-clés

Frontières intelligentes; Union européenne; Maroc; données biométriques; interopérabilité; protection des données; droits fondamentaux; coopération migratoire; externalisation; recours effectif.

LA PROYECCIÓN EXTERNA DE LAS FRONTERAS INTELIGENTES DE LA UNIÓN EUROPEA: DATOS BIOMÉTRICOS, COOPERACIÓN UE-MARRUECOS Y GARANTÍAS FUNDAMENTALES**Resumen**

Este artículo examina la proyección externa de las fronteras inteligentes de la Unión Europea a través de la cooperación migratoria con Marruecos. Partiendo de la transformación del control fronterizo en un régimen de identificación digital basado en sistemas de información, interoperabilidad y datos biométricos, el estudio analiza si dicha racionalidad puede producir efectos jurídicos fuera del espacio institucional de la Unión. El artículo no presume la existencia de un acceso marroquí directo a las bases europeas ni de un flujo generalizado de datos biométricos. Propone, más bien, una cartografía jurídica de las formas intermedias de circulación informacional: transferencia directa, acceso mediado, comunicación puntual, asistencia técnica a la identificación y externalización funcional del control. Esta distinción permite evaluar, mecanismo por mecanismo, las exigencias derivadas de la Carta de los Derechos Fundamentales, del derecho europeo de protección de datos y de los principios de legalidad, finalidad, necesidad, proporcionalidad, supervisión independiente y recurso efectivo. El caso UE-Marruecos muestra así que la cooperación migratoria solo puede ser jurídicamente admisible si sus efectos informacionales permanecen identificables, limitados y controlables.

Palabras clave

Fronteras inteligentes; Unión Europea; Marruecos; datos biométricos; interoperabilidad; protección de datos; derechos fundamentales; cooperación migratoria; externalización; recurso efectivo.

THE EXTERNAL PROJECTION OF THE EUROPEAN UNION'S SMART BORDERS: BIOMETRIC DATA, EU-MOROCCO COOPERATION AND FUNDAMENTAL RIGHTS SAFEGUARDS

Abstract

This article examines the external projection of the European Union's smart borders through migration cooperation with Morocco. It starts from the transformation of border control into a regime of digital identification based on large-scale information systems, interoperability and biometric data. The article does not presume that Moroccan authorities have direct access to EU databases, nor that a generalized flow of biometric data exists between the EU and Morocco. Instead, it proposes a legal mapping of intermediate forms of informational circulation: direct transfer, mediated access, targeted communication, technical assistance for identification and functional externalisation of control. This typology makes it possible to assess, mechanism by mechanism, the requirements arising from the Charter of Fundamental Rights, EU data protection law and the principles of legality, purpose limitation, necessity, proportionality, independent supervision and effective judicial protection. The EU-Morocco case shows that migration cooperation involving biometric rationalities cannot be justified by operational efficiency alone: it is legally admissible only where its informational effects are identifiable, limited, traceable and subject to effective safeguards.

Keywords

Smart borders; European Union; Morocco; biometric data; interoperability; data protection; fundamental rights; migration cooperation; externalisation; effective remedy.

SUMARIO

I. INTRODUCTION. II. LES FRONTIÈRES INTELLIGENTES DE L'UNION EUROPÉENNE COMME RÉGIME JURIDIQUE D'IDENTIFICATION NUMÉRIQUE: 1. La frontière intelligente comme construction normative du contrôle frontalier. 2. L'interopérabilité des systèmes et la centralité croissante de la biométrie. 3. De la surveillance du passage à la production d'une visibilité juridique des personnes en mobilité. III. LA COOPÉRATION MIGRATOIRE UE-MAROC À L'ÉPREUVE DE LA CIRCULATION DES DONNÉES BIOMÉTRIQUES ET DES GARANTIES FONDAMENTALES: 1. Le Maroc dans l'économie juridique de la coopération migratoire extérieure de l'Union. 2. Les formes possibles de circulation des données biométriques: transfert, accès indirect et externalisation fonctionnelle. 3. Les garanties fondamentales comme limite et condition de validité de la coopération biométrique. IV. CONCLUSION. BIBLIOGRAPHIE.

I. INTRODUCTION

La numérisation du contrôle migratoire ne transforme pas seulement les instruments de la frontière; elle modifie les conditions juridiques dans lesquelles la mobilité devient administrativement identifiable. Longtemps pensée comme une ligne territoriale et comme un moment de vérification documentaire, la frontière tend désormais à se déployer sous la forme d'une architecture informationnelle, fondée sur l'identification, la comparaison, la conservation et la circulation de données relatives aux personnes en mobilité (Mutlu *et al.*, 2025: 1-3).

Dans l'espace Schengen, cette évolution prolonge la dissociation entre la suppression des contrôles aux frontières intérieures et le renforcement des frontières extérieures. Elle s'appuie désormais sur une pluralité de systèmes d'information: SIS, VIS, Eurodac, EES et ETIAS auxquels s'ajoutent les mécanismes d'interopérabilité institués par les règlements de 2019, étant précisé que l'EES est déjà entré en fonctionnement complet tandis qu'ETIAS demeure en voie de déploiement².

L'intérêt juridique du sujet tient précisément à ce déplacement. La frontière intelligente ne constitue pas seulement une modernisation adminis-

² Commission européenne, «Entry/Exit System (EES) is fully operational», 10 avril 2026; Commission européenne, «The Entry/Exit System will become fully operational on 10 April 2026», 30 mars 2026.

trative du contrôle; elle organise un régime d'identification numérique des mobilités, dans lequel l'identité des personnes est produite par la mise en relation de données biographiques, documentaires, biométriques et historiques (Frowd, 2018: 1-6).

Cette transformation interne doit être replacée dans l'action extérieure migratoire de l'Union. La gestion européenne des mobilités ne s'exerce pas seulement aux frontières de l'espace Schengen; elle se prolonge à travers des partenariats avec des États tiers, des instruments financiers, des arrangements opérationnels, des mécanismes de réadmission, des coopérations policières et des dialogues politiques. Le Maroc occupe, dans cette architecture, une position particulière en raison de sa situation sur les routes de la Méditerranée occidentale et de l'Atlantique, mais aussi de la densité de sa coopération migratoire avec l'Union³.

Le cas marocain permet ainsi d'interroger la projection externe des frontières intelligentes européennes. Il ne s'agit pas de présumer que le Maroc disposerait d'un accès direct aux systèmes d'information de l'Union, ni qu'un transfert généralisé de données biométriques serait établi. L'enjeu est plus précis: déterminer si, entre l'absence d'accès direct et le transfert formel de données, des formes intermédiaires de circulation informationnelle peuvent apparaître à travers l'assistance technique, l'identification documentaire, la coopération consulaire, les retours, la réadmission ou la transmission de résultats d'identification.

La spécificité du cas marocain tient ainsi moins à l'existence démontrée d'un mécanisme unique de transmission biométrique qu'à la concentration, dans une même relation de coopération, de plusieurs instruments susceptibles de produire des effets informationnels. Le Maroc est à la fois un partenaire de voisinage, un État associé à la gestion des routes de la Méditerranée occidentale et de l'Atlantique, un bénéficiaire de programmes européens de soutien à la gestion migratoire, un acteur de la lutte contre le trafic de migrants et un interlocuteur dans les procédures d'identification, de retour et de réadmission. Cette superposition d'instruments permet de distinguer le cas marocain d'une hypothèse abstraite de coopération avec un État tiers: elle offre un terrain concret pour analyser la manière dont la rationalité européenne des frontières intelligentes peut se projeter sans nécessairement prendre la forme d'un accès direct aux bases de données de l'Union.

La difficulté juridique réside dans le caractère composite de cette coopération. L'action extérieure migratoire de l'Union se déploie rarement par un

³ Conseil de l'Union européenne, *Position of the European Union for the Association Council's Fifteenth Meeting*, doc. 5724/26, 30 janvier 2026, pp. 9-10.

instrument unique et pleinement formalisé; elle combine droit dérivé, soft law, financements, programmes opérationnels, coopération policière et arrangements pratiques. Cette fragmentation complique l'identification des bases juridiques applicables, des autorités responsables, des garanties exigibles et des voies de recours ouvertes aux personnes concernées (Nicolosi, 2024: 1-4).

En matière biométrique, cette fragmentation est particulièrement problématique. Les données biométriques ne sont pas de simples informations administratives: elles rattachent l'identité juridique au corps de la personne et peuvent produire des effets durables dans les procédures d'admission, de séjour, d'asile, de retour ou de réadmission (Strik, 2023: 908-910, 928-929). Leur traitement doit donc être apprécié au regard des articles 7, 8 et 47 de la Charte des droits fondamentaux, de l'article 16 TFUE, ainsi que des régimes européens de protection des données applicables aux institutions de l'Union, aux autorités nationales et, le cas échéant, aux transferts vers des États tiers (Hijmans, 2016).

Ce questionnement est renforcé par le Pacte européen sur la migration et l'asile, qui accentue l'articulation entre contrôle aux frontières, identification, enregistrement, procédures de retour, réforme d'Eurodac et partenariats internationaux. Dans ce contexte, la question n'est pas seulement de savoir si des données circulent matériellement entre l'Union et le Maroc; elle est de déterminer selon quelles formes une circulation informationnelle peut être juridiquement envisagée, avec quelles bases légales, sous quelles finalités, avec quelles garanties et sous quel contrôle.

Dans quelle mesure les frontières intelligentes de l'Union européenne peuvent-elles produire des effets externes dans la coopération migratoire avec un État tiers, en particulier le Maroc, sans porter une atteinte disproportionnée aux garanties fondamentales relatives à la vie privée, à la protection des données personnelles et au recours effectif.

Cette problématique se décline en trois interrogations. Il convient d'abord de préciser la qualification juridique de la frontière intelligente, afin de déterminer si elle relève d'une simple modernisation du contrôle frontalier ou d'un régime d'identification numérique des mobilités. Il faut ensuite distinguer les formes que peut prendre la circulation informationnelle dans la coopération UE-Maroc, entre transfert direct, accès médié, assistance technique, transmission d'un résultat d'identification et externalisation fonctionnelle. Il importe enfin d'apprécier les garanties fondamentales susceptibles d'encadrer ces mécanismes, notamment au regard de la légalité, de la finalité, de la proportionnalité, de la protection des données personnelles et de l'effectivité du recours.

L'hypothèse défendue est que la projection externe des frontières intelligentes ne se réduit pas à l'existence d'un transfert direct de données biométriques. Elle peut aussi résulter de mécanismes indirects — assistance technique, vérifi-

cation documentaire, transmission d'un résultat d'identification, coopération consulaire ou externalisation fonctionnelle — qui produisent des effets juridiques sur les personnes concernées. Dès lors, l'absence d'accès direct d'un État tiers aux bases européennes ne suffit pas à exclure l'application d'exigences strictes de légalité, de finalité, de nécessité, de proportionnalité, de supervision et de recours effectif (Faustini Torres, 2026: 677-683, 692-697).

La méthode retenue est doctrinale, normative et critique. Elle repose sur l'analyse du droit primaire et dérivé de l'Union relatif aux frontières, à l'interopérabilité, à la biométrie et à la protection des données, ainsi que sur l'examen des instruments politiques, financiers et opérationnels structurant la coopération UE-Maroc. L'étude ne vise pas à établir empiriquement l'existence d'un flux déterminé de données biométriques; elle propose une grille de qualification juridique permettant de distinguer les formes possibles de circulation informationnelle, leurs degrés d'intensité et les garanties qui doivent les conditionner.

L'article se déploie en deux temps. Il montre d'abord que les frontières intelligentes européennes constituent un régime juridique d'identification numérique, structuré par l'interopérabilité des systèmes d'information et par la centralité de la biométrie. Il examine ensuite la projection externe de cette rationalité informationnelle dans la coopération UE-Maroc, en distinguant les formes possibles de circulation ou d'usage des données biométriques et les garanties fondamentales qui doivent en conditionner la validité.

II. LES FRONTIÈRES INTELLIGENTES DE L'UNION EUROPÉENNE COMME RÉGIME JURIDIQUE D'IDENTIFICATION NUMÉRIQUE

L'analyse de la projection externe des frontières intelligentes suppose d'abord de préciser leur qualification en droit de l'Union. Ces dispositifs ne relèvent pas d'une simple modernisation technique du contrôle frontalier: ils organisent un régime d'identification numérique des ressortissants de pays tiers, structuré par les systèmes d'information européens, les mécanismes d'interopérabilité et l'usage croissant de données biométriques. Cette première partie examine donc la frontière intelligente comme construction normative, avant d'analyser l'interopérabilité des systèmes et la production d'une visibilité juridique des personnes en mobilité.

1. LA FRONTIÈRE INTELLIGENTE COMME CONSTRUCTION NORMATIVE DU CONTRÔLE FRONTALIER

La frontière intelligente ne peut être réduite à une simple modernisation technique du contrôle frontalier. Elle traduit une transformation juridique de

la frontière, qui n'est plus seulement un lieu physique de vérification documentaire, mais un ensemble d'opérations normativement organisées: collecte de données, vérification documentaire, identification biométrique, comparaison avec des fichiers, appréciation du risque, conservation des traces et réutilisation possible des informations.

Cette transformation ne supprime pas la frontière territoriale; elle la prolonge par une frontière informationnelle. Ce prolongement est juridique autant que technique, car les textes de l'Union autorisent la collecte des données, déterminent les finalités du traitement, désignent les autorités compétentes, organisent les conditions d'accès aux systèmes et prévoient les garanties applicables aux personnes concernées. Le droit ne se borne donc pas à limiter la technologie après coup; il participe à la constitution même de la frontière intelligente (Jeandesboz, 2016: 292-309).

Cette mutation est particulièrement visible dans l'espace européen. Le «système intégré de gestion des frontières extérieures» de l'Union repose désormais sur un usage intensif des technologies numériques. Frédérique Michéa souligne que le projet européen de frontières intelligentes s'inscrit dans une logique de filtrage permanent des ressortissants de pays tiers se présentant aux frontières extérieures, les fichiers numériques occupant une place centrale dans cette organisation du contrôle (Michéa, 2020: 37-63). L'enjeu n'est donc plus seulement d'empêcher ou d'autoriser un passage. Il est de rendre les mobilités lisibles, vérifiables et administrativement traitables avant même que l'autorité ne prenne une décision individuelle.

La notion de filtrage est ici essentielle. Elle permet de comprendre que la frontière intelligente ne se contente pas de surveiller: elle distingue, classe et hiérarchise les mobilités. Certaines circulations sont fluidifiées parce qu'elles apparaissent régulières, documentées et compatibles avec les catégories administratives existantes; d'autres sont ralenties, suspectées ou empêchées parce qu'elles sont perçues comme incertaines, insuffisamment documentées ou porteuses d'un risque migratoire, sécuritaire ou identitaire. La frontière cesse ainsi d'être seulement un point de contrôle pour devenir un processus de gouvernement: elle se déploie avant le départ, au moment du franchissement, pendant le séjour, lors de la sortie et, le cas échéant, dans les procédures d'identification ou de retour.

Dans cette logique, la personne en mobilité n'est plus seulement appréhendée comme le titulaire d'un document de voyage. Elle devient également un ensemble de données d'identité, de données documentaires, de données biométriques et de traces de circulation. La mobilité est ainsi convertie en information juridiquement exploitable.

L'automatisation accentue encore cette évolution⁴. Les travaux récents consacrés au «techno-contrôle des migrations» montrent que les systèmes d'intelligence artificielle et les outils automatisés sont désormais mobilisés dans le contrôle des frontières, la détection de mouvements, la reconnaissance faciale, la prédiction de déplacements humains ou encore l'aide à l'examen administratif de certaines demandes (Sibley et Chappart, 2024a: 11-14). Ces dispositifs ne remplacent pas nécessairement la décision humaine, mais ils la préparent, l'orientent ou la préstructurent. Le pouvoir frontalier ne disparaît donc pas derrière la machine; il se recompose à travers des infrastructures techniques qui orientent les conditions de production de la décision administrative.

Cette médiation technique rend le pouvoir frontalier moins immédiatement perceptible. Dans le modèle classique, la personne contrôlée pouvait identifier l'agent, le lieu du contrôle et la décision prise. Dans le modèle intelligent, une partie du contrôle s'opère par l'interrogation de systèmes d'information, le rapprochement de données, la détection d'incohérences ou la production de signalements automatisés ou semi-automatisés (de Terwangne, 2020: 97-116). La décision demeure formellement administrative, mais elle est préparée par une infrastructure informationnelle qui en conditionne les possibilités. La frontière intelligente doit donc être comprise comme une catégorie juridique de gouvernement: elle ne modifie pas seulement les moyens du contrôle, mais sa rationalité même, en déplaçant l'action publique du passage vers l'identité, du territoire vers la donnée et du moment frontalier vers un processus continu d'identification (Sibley et Chappart, 2024b: 3-6).

La frontière intelligente ne met donc pas fin à la souveraineté frontalière; elle en transforme les instruments. La puissance publique ne s'exprime plus seulement par la décision d'admission, de refus ou de contrôle matériel du passage, mais aussi par la maîtrise des infrastructures d'identification et des circuits de données.

Une telle reconfiguration appelle une analyse juridique exigeante. Dès lors que la frontière intelligente repose sur la collecte, la conservation et l'exploitation de données relatives aux personnes, elle ne peut être appréciée uniquement au regard de son efficacité opérationnelle. Elle doit être soumise aux exigences de légalité, de finalité, de nécessité, de proportionnalité, de transparence et d'effectivité des garanties.

⁴ Règlement (UE) 2024/1689 du Parlement européen et du Conseil, du 13 juin 2024, établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L, 2024/1689, 12 juillet 2024, art. 6 et annexe III, point 7.

Ainsi comprise, la frontière intelligente ne constitue pas un simple perfectionnement de la frontière classique. Elle déplace le contrôle du territoire vers la donnée, du passage vers l'identité, du moment frontalier vers le processus informationnel. Cette catégorie ne prend toutefois toute sa consistance qu'à travers l'architecture qui la rend opératoire: l'interopérabilité des systèmes d'information européens et la centralité croissante de la biométrie.

2. L'INTEROPÉRABILITÉ DES SYSTÈMES ET LA CENTRALITÉ CROISSANTE DE LA BIOMÉTRIE

L'interopérabilité constitue le noyau normatif et technique des frontières intelligentes européennes. Elle ne désigne pas seulement la capacité de plusieurs systèmes informatiques à communiquer entre eux. En droit de l'Union européenne, elle renvoie à une architecture organisée permettant l'interrogation coordonnée de systèmes d'information initialement distincts, la production de correspondances et le renforcement de l'identification des personnes concernées. La logique n'est donc plus celle d'une consultation isolée de fichiers séparés, mais celle d'un environnement intégré dans lequel les données relatives aux ressortissants de pays tiers peuvent être recherchées, rapprochées et exploitées selon des droits d'accès juridiquement déterminés⁵.

Cette évolution répond à une difficulté structurelle du modèle antérieur. L'Union européenne a progressivement construit plusieurs systèmes d'information à grande échelle, chacun conçu autour d'une finalité particulière: le système d'information Schengen pour les signalements, le système d'information sur les visas pour la politique commune des visas, Eurodac pour la comparaison des empreintes digitales dans le cadre du régime Dublin, l'EES pour l'enregistrement des entrées et sorties, et ETIAS pour l'autorisation préalable de voyage des ressortissants de pays tiers exemptés de visa. Cette multiplication des instruments a donné naissance à un paysage fragmenté, composé de bases de données spécialisées, créées à des moments différents, sur des fondements juridiques distincts et selon des logiques institutionnelles propres (Blasi Casagran, 2021: 433-435).

⁵ 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'Union dans le domaine des frontières et des visas, JOUE L 135, 22 mai 2019, p. 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'Union dans le domaine de la coopération policière et judiciaire, de l'asile et de la migration, JOUE L 135, 22 mai 2019, p. 85; Commission européenne, «Interoperability», DG Migration and Home Affairs.

La doctrine a bien identifié cette fragmentation. Frédérique Michéa observe que les instruments opérationnels régissant la collecte, le stockage et l'échange des données personnelles des personnes migrantes forment un « kaléidoscope » de systèmes d'information à grande échelle. Cette image est particulièrement pertinente: chaque système possède sa fonction, mais l'ensemble produit une architecture complexe de surveillance, d'identification et de gestion des mobilités (Michéa, 2020: 37-63). L'interopérabilité apparaît alors comme une réponse à cette dispersion. Elle vise à éviter que les données demeurent enfermées dans des silos techniques et juridiques, tout en permettant aux autorités compétentes d'accéder plus efficacement aux informations nécessaires à l'identification, au contrôle et à la gestion des risques.

Le règlement (UE) 2019/817 institue le cadre d'interopérabilité dans le domaine des frontières et des visas, tandis que le règlement (UE) 2019/818 organise un cadre parallèle dans les domaines de la coopération policière et judiciaire, de l'asile et de la migration. Cette dualité s'explique par la diversité des bases juridiques et des systèmes concernés. Certains instruments relèvent du développement de l'acquis Schengen, comme le SIS, le VIS, l'EES et ETIAS; d'autres, notamment Eurodac et ECRIS-TCN, n'en relèvent pas selon les mêmes modalités⁶. L'interopérabilité ne signifie donc pas fusion indifférenciée des fichiers, mais construction d'une couche transversale permettant leur interrogation coordonnée, sous réserve du respect des finalités assignées et des droits d'accès juridiquement prévus.

Cette précision est essentielle: l'interopérabilité ne supprime pas juridiquement les systèmes existants; elle les relie. Elle ne confère pas nécessairement à chaque autorité un accès général à toutes les données, mais elle modifie les conditions du contrôle en permettant de vérifier plus rapidement si une identité, un document, une empreinte ou une image faciale se rattache à des données déjà enregistrées dans plusieurs systèmes. C'est précisément cette capacité transversale qui nourrit les critiques doctrinales. Niovi Vavoula souligne que les règlements d'interopérabilité soulèvent des préoccupations majeures en matière de vie privée et de protection des données personnelles des ressortissants de pays tiers (Vavoula, 2020: 131-156), tandis qu'Evelien Brouwer montre que l'extension progressive des finalités des grandes bases européennes tend à brouiller la ligne séparant contrôle migratoire, sécurité et répression pénale (Brouwer, 2020: 71-92). L'interopérabilité n'est donc pas seulement une rationalisation technique; elle déplace les frontières entre droit

⁶ Commission européenne, «Interoperability», DG Migration and Home Affairs, mise à jour du 13 octobre 2025.

des visas, droit des frontières, droit de l'asile, coopération policière et droit de la protection des données.

L'architecture européenne repose principalement sur quatre composants: le portail de recherche européen, le service partagé de mise en correspondance biométrique, le répertoire commun de données d'identité et le détecteur d'identités multiples⁷. Ces composants ne remplissent pas la même fonction, mais ils contribuent tous à une même finalité: consolider l'identification des personnes et rendre plus efficaces les contrôles aux frontières extérieures de l'Union.

Le portail de recherche européen, ou European Search Portal, fonctionne comme un point d'interrogation unique. Il permet aux autorités habilitées d'effectuer une recherche simultanée dans plusieurs systèmes d'information européens et, dans certains cas, dans les données d'Europol, conformément aux droits d'accès reconnus à chaque autorité. Sa fonction n'est pas de fusionner les systèmes, mais de simplifier leur consultation. L'effet juridique est toutefois significatif: l'autorité ne se trouve plus face à une succession de fichiers séparés; elle dispose d'une capacité de recherche transversale qui modifie les conditions concrètes du contrôle⁸.

Le service partagé de mise en correspondance biométrique, ou shared Biometric Matching Service, occupe une place encore plus décisive. Il constitue le cœur biométrique de l'interopérabilité. Mis en service par eu-LISA en mai 2025, il permet de stocker et de comparer des données biométriques, notamment des empreintes digitales et des images faciales, à travers plusieurs systèmes européens. La Commission européenne présente ce système comme une infrastructure appelée à contenir environ 400 millions de modèles biométriques et permettant, pour la première fois à cette échelle, l'usage de la reconnaissance faciale dans un cadre d'identification transversale⁹. La biométrie devient ainsi le langage commun de l'architecture interopérable.

Cette centralité biométrique modifie la nature du contrôle. Dans le contrôle documentaire classique, l'administration vérifie l'authenticité ou la validité d'un document. Dans le contrôle biométrique interopérable, elle vérifie la correspondance entre un corps, une identité déclarée et des données déjà présentes dans plusieurs systèmes. La jurisprudence de la Cour de justice

⁷ Règlement (UE) 2019/817, préc.; Commission européenne, «Interoperability», préc.

⁸ Commission européenne, «Interoperability», préc.

⁹ eu-LISA, «First Interoperability Milestone Achieved: sBMS and VIS4EES Go Live», communiqué, 21 mai 2025; Commission européenne, «Commission Announces Launch of the Shared Biometric Matching Service», 19 mai 2025.

confirme que l'usage de données biométriques à des fins d'identification constitue une ingérence dans les droits garantis par les articles 7 et 8 de la Charte, mais que cette ingérence peut être admise lorsqu'elle poursuit une finalité légitime, telle que la sécurité documentaire ou la prévention de la fraude à l'identité, et lorsqu'elle respecte le principe de proportionnalité. Dans l'arrêt *Schwarz*, la Cour a ainsi apprécié l'enregistrement des empreintes digitales dans les passeports biométriques au regard de la finalité d'identification et de sécurisation des documents de voyage¹⁰. Cette approche a été prolongée dans l'arrêt *R.L. c. Landeshauptstadt Wiesbaden*, où la Cour a examiné la validité de l'obligation d'intégrer deux empreintes digitales dans les cartes d'identité des citoyens de l'Union, notamment au regard des articles 7 et 8 de la Charte et de l'article 35 du RGPD¹¹. Le corps devient alors un point d'ancrage de l'identité numérique: l'empreinte digitale et l'image faciale permettent de stabiliser l'identification là où les données alphanumériques peuvent être incertaines, mal orthographiées, translittérées différemment ou manipulées. Cette fonction explique la valeur opérationnelle de la biométrie, mais aussi son intensité juridique: l'identification ne porte plus seulement sur un document; elle porte directement sur des caractéristiques corporelles traitées comme données personnelles sensibles.

Matija Kontak rappelle, à propos des politiques biométriques envisagées par Frontex, que ces technologies ne sont pas de simples instruments d'efficacité administrative: elles produisent des effets sur les droits fondamentaux, notamment la vie privée et la protection des données personnelles (Kontak, 2024: 621-640). Cette observation vaut plus encore dans une architecture interopérable, où la donnée biométrique n'est pas collectée pour une vérification ponctuelle, mais peut devenir un point de comparaison transversal entre plusieurs systèmes.

Le troisième composant, le Common Identity Repository, correspond au répertoire commun de données d'identité. Il conserve les données nécessaires à l'identification des personnes lorsque celles-ci sont déjà présentes dans l'un des systèmes sous-jacents. Il comprend notamment des données d'identité, des données relatives au document de voyage et des données biométriques, les modèles biométriques correspondants étant conservés dans le service partagé de mise en correspondance biométrique. Le CIR ne doit donc pas être compris comme une simple base supplémentaire; il fonctionne comme un espace

¹⁰ CJUE, 17 octobre 2013, Michael Schwarz c. Stadt Bochum, C-291/12, ECLI:EU:C:2013:670.

¹¹ CJUE, grande chambre, 21 mars 2024, R.L. c. Landeshauptstadt Wiesbaden, C-61/22, ECLI:EU:C:2024:251.

commun d'identification, destiné à faciliter la reconnaissance d'une personne déjà enregistrée dans plusieurs systèmes¹².

Le quatrième composant, le Multiple-Identity Detector, vise la détection des identités multiples. Sa fonction consiste à créer et conserver des liens entre les données présentes dans les systèmes à grande échelle afin de détecter les identités multiples. L'objectif officiel est double: faciliter les contrôles des voyageurs de bonne foi et lutter contre la fraude à l'identité. Mais ce mécanisme soulève une difficulté juridique importante: l'existence de plusieurs identités administratives ne traduit pas nécessairement une fraude. Elle peut résulter de différences de transcription, de translittérations variables, d'erreurs administratives, de changements d'état civil ou de contextes documentaires nationaux. C'est pourquoi le droit de l'Union prévoit des garanties destinées à éviter les décisions défavorables ou discriminatoires à l'encontre des personnes disposant de plusieurs identités légitimes¹³.

L'interopérabilité modifie ainsi la structure juridique du contrôle frontalier. L'autorité ne vérifie plus seulement un passage, un visa ou un document; elle interroge une architecture d'identité, capable de consolider les données disponibles ou, au contraire, de faire apparaître une incohérence. L'autorité compétente ne cherche plus seulement à savoir si un passeport est valide ou si une personne fait l'objet d'un signalement; elle cherche à établir si l'identité présentée est cohérente avec les données conservées dans différents systèmes. La frontière intelligente devient alors un espace d'agrégation et de comparaison. Elle produit une identité consolidée, ou au contraire une suspicion d'incohérence, à partir du croisement de données auparavant séparées.

Cette évolution renforce le risque de glissement des finalités. Le principe de limitation des finalités impose que les données soient collectées pour des objectifs déterminés, explicites et légitimes, et qu'elles ne soient pas traitées ultérieurement d'une manière incompatible avec ces objectifs. Or l'interopérabilité accroît précisément la disponibilité, la recherchabilité et la réutilisabilité des données. Hartmut Aden considère que l'interconnexion des bases policières et migratoires constitue un changement de paradigme pour le principe de limitation des finalités, dans la mesure où des systèmes créés pour des objectifs distincts peuvent être mobilisés dans des logiques plus larges d'identification et de sécurité (Aden, 2020: 93-108).

L'exemple d'Eurodac illustre cette difficulté. Conçu initialement pour faciliter l'application du système Dublin par la comparaison des

¹² Règlement (UE) 2019/817, préc., art. 17 et s.; Commission européenne, «Interoperability», préc.

¹³ Commission européenne, «Interoperability», préc.

empreintes digitales, Eurodac a progressivement acquis une dimension répressive. Laurent Rousvoal montre que ce fichier européen procède du croisement de nouvelles finalités dans le cadre d'un basculement de la politique migratoire vers un paradigme sécuritaire. Sa refonte de 2013 a notamment ouvert l'accès aux autorités répressives pour la lutte contre certaines formes graves de criminalité et le terrorisme. Le cas d'Eurodac montre ainsi comment une base de données initialement liée à l'asile peut être réorientée vers des finalités de sécurité intérieure (Rousvoal, 2020: 81-94).

Cette tension n'est pas marginale. Elle se trouve au cœur du projet d'interopérabilité. Cristina Blasi Casagran souligne que les règlements de 2019 ont interconnecté des bases créées pour des finalités de sécurité et de gestion des frontières, en vue de prévenir l'immigration irrégulière et d'améliorer la sécurité dans l'espace de liberté, de sécurité et de justice. Elle relève que cette interconnexion soulève des difficultés sérieuses au regard des droits fondamentaux garantis par la Charte de l'Union européenne, notamment la protection des données, les droits de l'enfant, la non-discrimination, la nécessité et la proportionnalité. L'interopérabilité n'est donc pas seulement un enjeu de performance administrative; elle appelle un contrôle rigoureux au regard des exigences de l'État de droit et des droits fondamentaux (Blasi Casagran, 2021: 433-457).

La question de la conservation des données renforce cette analyse. L'efficacité de l'interopérabilité dépend largement de la possibilité de conserver les données suffisamment longtemps pour les comparer, les retrouver et les exploiter. Mais plus la durée de conservation est longue, plus le contrôle devient profond dans le temps. Maryline Boizard rappelle que les données permettant d'identifier les migrants sont collectées depuis plusieurs années par différents systèmes automatisés d'information, notamment le SIS, le VIS et Eurodac. Elle souligne également que, dans le cadre de l'EES, les données sont en principe conservées trois ans, mais peuvent l'être cinq ans en l'absence de fiche de sortie après l'expiration de la période autorisée, ce qui avait suscité des réserves du Contrôleur européen de la protection des données au regard de la proportionnalité. La durée de conservation n'est donc pas un détail technique; elle détermine l'étendue temporelle de la visibilité administrative (Boizard, 2020: 117-126).

La montée en puissance d'eu-LISA confirme enfin que l'interopérabilité est aussi une architecture institutionnelle. Chargée de la gestion opérationnelle des systèmes d'information à grande échelle dans l'espace de liberté, de sécurité et de justice, l'agence occupe une place centrale dans le fonctionnement des frontières intelligentes. Celles-ci ne reposent donc pas seulement sur les autorités nationales; elles sont également structurées par des systèmes

communs, des standards techniques et une administration européenne des infrastructures numériques (Billet, 2020: 65-79).

Cette institutionnalisation technique prépare également l'articulation avec l'intelligence artificielle. Niovi Vavoula montre que l'interopérabilité des grands systèmes européens et le déploiement de l'IA dans les domaines de la migration, de l'asile et de la gestion des frontières ne doivent pas être étudiés séparément. Certains composants d'interopérabilité peuvent devenir des prérequis ou des facilitateurs de traitements plus automatisés, plus prédictifs et plus difficiles à contrôler (Vavoula, 2024: 1228-1249).

Cette évolution confirme l'ambivalence des frontières intelligentes. L'interopérabilité peut améliorer l'exactitude de l'identification, réduire certaines fraudes documentaires et renforcer la cohérence de l'action administrative. Mais elle peut aussi intensifier la surveillance des ressortissants de pays tiers, accroître les risques d'erreur, compliquer l'exercice des droits d'accès et de rectification, et favoriser des usages secondaires éloignés de la finalité initiale. Cette ambivalence montre que l'architecture interopérable doit être appréciée autant au regard de son efficacité que de ses effets sur les droits fondamentaux (La Spina, 2026).

Il en résulte que l'interopérabilité et la biométrie ne sont pas de simples accessoires des frontières intelligentes. Elles en constituent l'armature juridique et opérationnelle. L'interopérabilité fournit la structure permettant la circulation, le rapprochement et la consolidation des données; la biométrie fournit le point d'ancrage corporel de l'identité numérique. Ensemble, elles transforment le contrôle frontalier en contrôle d'architecture: l'autorité ne vérifie plus seulement une personne à un point de passage, mais une identité dans un écosystème de données. Cette mutation prépare le passage de la surveillance du franchissement à la production d'une visibilité juridique continue des personnes en mobilité.

Cette spécificité apparaît plus nettement lorsque la coopération UE-Maroc est rapportée à ses points d'application opérationnels. Le Maroc n'est pas seulement mentionné comme un voisin méridional de l'Union ou comme un partenaire général de dialogue migratoire; il est situé au croisement de plusieurs chaînes concrètes d'action publique: surveillance et gestion des routes de la Méditerranée occidentale et de l'Atlantique, lutte contre les réseaux de passeurs, appui européen aux capacités nationales de gestion des frontières, coopération avec les agences européennes, identification des personnes en situation irrégulière, délivrance éventuelle de documents de voyage et organisation des retours. C'est dans cette pluralité de séquences administratives et opérationnelles que peut se former une circulation informationnelle juridiquement pertinente, même en l'absence d'accès direct du Maroc aux systèmes européens d'information.

3. DE LA SURVEILLANCE DU PASSAGE À LA PRODUCTION D'UNE VISIBILITÉ JURIDIQUE DES PERSONNES EN MOBILITÉ

L'interopérabilité des systèmes et la centralité de la biométrie conduisent à dépasser une conception ponctuelle du contrôle frontalier. La frontière intelligente ne se borne plus à surveiller le moment du passage; elle organise un suivi informationnel de la mobilité, depuis l'anticipation du déplacement jusqu'à l'enregistrement de l'entrée, la conservation de l'historique, la vérification de l'identité et la mobilisation ultérieure des traces produites par la circulation. L'enjeu n'est donc plus seulement de savoir qui franchit la frontière, avec quel document et dans quelles conditions, mais de déterminer qui est identifiable, recoupable, retrouvable, comparable ou signalable dans un environnement informationnel intégré. La frontière produit ainsi une visibilité juridique de la personne en mobilité, c'est-à-dire une capacité institutionnelle à la connaître, à la qualifier et à la réinscrire dans une chaîne de décision.

Cette visibilité n'est pas une simple conséquence technique de la numérisation; elle résulte d'une construction juridique. Les systèmes d'information européens ne produisent pas seulement des données: ils les rendent recevables, consultables et mobilisables par des autorités habilitées. Ils transforment des éléments de déplacement: entrée, sortie, autorisation, refus, signalement, empreinte, image faciale ou document de voyage en unités administratives susceptibles de fonder ou d'orienter une décision. La donnée devient ainsi un instrument de juridicisation de la mobilité.

Cette logique rejoint l'analyse de Frédérique Michéa, selon laquelle le système intégré de gestion des frontières extérieures de l'Union repose sur un usage intensif des technologies numériques et sur la démultiplication des points de contrôle à l'égard des ressortissants de pays tiers. La frontière intelligente ne se limite donc pas au poste-frontière: elle disperse le contrôle dans une pluralité d'espaces informationnels où une donnée peut établir, vérifier ou contester une identité mobile (Michéa, 2020: 37-63).

Le passage du contrôle ponctuel au suivi informationnel repose d'abord sur l'enregistrement. En enregistrant les entrées, les sorties, les refus d'entrée, les demandes d'autorisation ou les données biométriques, les systèmes européens donnent à la mobilité une mémoire administrative. Le déplacement ne disparaît plus avec l'acte de franchissement; il laisse une trace conservée, susceptible d'être réutilisée pour vérifier la durée du séjour, détecter un dépassement, identifier une personne ou reconstruire un parcours. Comme le montre Maryline Boizard, l'enjeu juridique ne tient donc pas seulement à la collecte initiale des données, mais aussi à leur durée de conservation dans les systèmes automatisés d'information. Dans cette perspective, la durée de

conservation n'est pas un simple paramètre technique: elle détermine la profondeur temporelle de la visibilité administrative.

Cette mémoire informationnelle transforme également la notion d'identité frontalière. L'identité ne se limite plus au nom, à la nationalité ou au document présenté; elle se construit par accumulation de données biographiques, biométriques et historiques. Elle devient une identité administrative consolidée, produite par la mise en relation de fragments d'information issus de plusieurs systèmes.

Cette consolidation peut renforcer l'efficacité du contrôle, mais elle accroît aussi la dépendance de la personne à la qualité des données. Une erreur d'enregistrement, une translittération divergente, une donnée biométrique mal associée ou un signalement inexact peuvent produire des effets juridiques importants. La visibilité produite par les systèmes n'est donc pas nécessairement synonyme de vérité; elle peut aussi constituer une vérité administrative partielle, contestable ou difficilement réversible (Argyriou et Leese, 2026).

La notion de profilage doit toutefois être introduite avec prudence. La frontière intelligente n'implique pas nécessairement un profilage généralisé au sens strict, mais elle repose sur des mécanismes de catégorisation: voyageur régulier, personne exemptée de visa, demandeur de protection internationale, personne signalée, identité incertaine, dépassement de séjour ou risque migratoire. Ces catégories orientent les décisions administratives et peuvent conduire à des contrôles différenciés. La mobilité produit ainsi des traces juridiquement exploitables: une entrée enregistrée peut servir à calculer une durée de séjour; une absence de sortie peut fonder une suspicion de dépassement; une empreinte digitale peut permettre une identification ultérieure; un document numérique peut être confronté à une déclaration administrative ou contentieuse. La trace n'est donc pas une simple information conservée: elle devient un élément susceptible d'orienter la qualification juridique de la personne (Sibley et Chappart, 2024b: 3-6).

Cette logique peut se prolonger jusque dans le contentieux. Thibaut Fleury Graff montre, à propos de la preuve numérique en matière d'asile, que les documents numériques, publications en ligne ou éléments issus des réseaux sociaux peuvent nourrir l'appréciation juridictionnelle, sous réserve du respect du contradictoire et des exigences de crédibilité (Fleury Graff, 2020: 175-187). Cette observation confirme que la visibilité numérique ne produit pas seulement des effets administratifs; elle peut aussi devenir matière à discussion juridictionnelle.

La production de visibilité juridique affecte ainsi la manière dont les personnes en mobilité deviennent administrativement traitables (Pelizza *et al.*, 2024: 207-215). L'enregistrement, la comparaison et la conservation des données permettent de rattacher une personne à un dossier, à une identité, à

un historique, à une autorisation ou à un signalement. Cette visibilité peut faciliter l'accès à certains droits lorsqu'elle permet d'établir une identité ou de documenter une situation; elle peut aussi renforcer le contrôle lorsque la personne devient plus facilement localisable, comparable ou éloignable. C'est pourquoi la question juridique centrale n'est pas celle de l'efficacité technique du traitement, mais celle de ses finalités, de sa transparence, de sa proportionnalité et des garanties permettant à la personne concernée de comprendre, contester ou rectifier les effets produits par les systèmes (Leese *et al.*, 2022: 5-25).

La visibilité juridique n'est donc pas nécessairement illégitime. Elle peut être nécessaire à l'administration régulière des mobilités, à la sécurité documentaire et, parfois, à l'accès effectif à certaines protections. Elle devient toutefois problématique lorsqu'elle dépasse sa finalité initiale, lorsqu'elle repose sur des systèmes opaques ou lorsqu'elle ne s'accompagne pas de droits effectifs d'information, d'accès, de rectification et de recours. La frontière intelligente apparaît ainsi comme un dispositif à double face: elle rend les parcours plus lisibles et les décisions plus traçables, mais elle peut aussi transformer la mobilité en dossier permanent. Ce constat permet de passer à la seconde partie: lorsque cette visibilité est projetée dans la coopération avec des États tiers, notamment le Maroc, la question devient celle de la circulation directe ou indirecte des données biométriques et des garanties capables d'en encadrer les usages (Amoore, 2020).

La frontière intelligente apparaît alors comme un dispositif à double face. D'un côté, elle permet une meilleure continuité administrative: elle rend les parcours plus lisibles, les identités plus vérifiables et les décisions plus traçables (De Terwangne, 2020: 97-116). De l'autre, elle peut intensifier le gouvernement informationnel des personnes en mobilité en rendant chaque déplacement, chaque autorisation, chaque refus et chaque incohérence potentiellement réutilisable. La mobilité devient un dossier en mouvement. La personne n'est plus seulement contrôlée parce qu'elle franchit une frontière; elle est gouvernée parce qu'elle laisse des traces dans des systèmes qui rendent son parcours administrativement disponible.

Cette analyse permet de conclure la première partie. La frontière intelligente n'est pas seulement un perfectionnement du contrôle frontalier; elle produit une visibilité juridique continue des personnes en mobilité. Cette visibilité repose sur l'enregistrement, l'historique, l'identification biométrique, la comparaison des données et la réutilisation possible des traces dans différents contextes administratifs ou contentieux. Elle rend possible l'intensification du gouvernement informationnel des frontières, tout en révélant les risques de glissement des finalités, d'opacité des traitements et d'affaiblissement des garanties individuelles. C'est précisément ici que s'opère le passage vers la

seconde partie: lorsque cette visibilité est projetée dans la coopération migratoire avec des États tiers, notamment le Maroc, la question devient celle de la circulation directe ou indirecte des données biométriques et des conditions juridiques capables d'en encadrer les usages.

III. LA COOPÉRATION MIGRATOIRE UE-MAROC À L'ÉPREUVE DE LA CIRCULATION DES DONNÉES BIOMÉTRIQUES ET DES GARANTIES FONDAMENTALES

La projection externe des frontières intelligentes ne peut être appréciée à partir de la seule densité de la coopération migratoire. Elle suppose d'identifier les formes concrètes par lesquelles les données, les résultats d'identification ou les capacités biométriques peuvent circuler entre l'Union et le Maroc, directement ou indirectement, puis d'en mesurer la compatibilité avec les garanties fondamentales. Cette seconde partie situe d'abord le Maroc dans l'économie juridique de la coopération migratoire extérieure de l'Union, avant de distinguer les mécanismes possibles de circulation informationnelle et d'examiner les conditions de validité qui découlent de la protection des données, de la vie privée et du droit au recours effectif.

1. LE MAROC DANS L'ÉCONOMIE JURIDIQUE DE LA COOPÉRATION MIGRATOIRE EXTÉRIEURE DE L'UNION

Après avoir montré que la frontière intelligente européenne transforme le contrôle des mobilités en une gouvernance informationnelle fondée sur l'identification, l'interopérabilité et la production de visibilité juridique, il convient d'examiner la manière dont cette rationalité peut se projeter au-delà de l'espace institutionnel de l'Union. La coopération migratoire UE-Maroc constitue, à cet égard, un terrain particulièrement révélateur. Elle ne se réduit ni à une relation bilatérale classique, ni à une assistance technique ponctuelle; elle s'inscrit dans une économie juridique composite, où se superposent instruments politiques, financements européens, coopération opérationnelle, dialogue sécuritaire, lutte contre le trafic de migrants et dispositifs de retour ou de réadmission (Gazzotti *et al.*, 2023: 70-72, 75-79).

Cette centralité ne tient pas seulement à la géographie. Certes, le Maroc occupe une position stratégique dans l'espace euro-africain: État d'origine, de transit et de destination, il se situe au croisement de la route de la Méditerranée occidentale, de la route atlantique vers les îles Canaries, des mobilités subsahariennes et des dynamiques migratoires nord-africaines. Mais l'importance du Maroc dans la politique migratoire européenne résulte surtout de la

densité des instruments qui structurent sa relation avec l'Union. Depuis l'accord d'association entré en vigueur en 2000, puis le statut avancé et la politique européenne de voisinage, la migration est progressivement devenue l'un des champs les plus sensibles du partenariat euro-marocain. La déclaration conjointe établissant le partenariat pour la mobilité de 2013 a confirmé cette évolution en inscrivant la coopération dans une approche globale articulant mobilité légale, migration et développement, lutte contre l'immigration irrégulière, trafic de migrants, traite des êtres humains, retour, réadmission et protection internationale¹⁴.

Cette architecture montre que la coopération migratoire UE-Maroc relève d'abord d'un droit souple et partenarial. Le partenariat pour la mobilité ne constitue pas un traité créateur d'obligations internationales directement opposables; il organise plutôt un cadre politique de dialogue, de coordination et de programmation. Cette caractéristique est décisive. Elle permet à l'Union d'inscrire la migration dans une relation durable avec le Maroc sans passer nécessairement par un accord international complet, juridiquement contraignant, couvrant l'ensemble des dimensions de la coopération migratoire. La déclaration de 2013 précise d'ailleurs que ses dispositions ne sont pas destinées à créer des droits ou obligations en droit international. L'intérêt juridique du dispositif ne tient donc pas à sa force obligatoire au sens classique, mais à sa capacité de produire des effets de structuration: il identifie des priorités, associe des agences européennes, organise des canaux de coopération et inscrit la gestion migratoire dans une logique de dialogue permanent¹⁵.

Cette souplesse instrumentale est caractéristique de la dimension externe de la politique migratoire européenne. Dans ce domaine, l'Union n'agit pas uniquement par la voie des accords formels. Elle mobilise également des partenariats, des plans d'action, des instruments financiers, des programmes régionaux, des arrangements opérationnels et des mécanismes d'incitation. La doctrine a montré que cette externalisation ne peut être comprise comme une simple délégation du contrôle migratoire à des États tiers. Elle correspond davantage à une redistribution des fonctions de gouvernance: l'Union conserve la maîtrise de ses objectifs politiques et financiers, tandis que les États partenaires, dont le Maroc, participent à la mise en œuvre concrète de certaines fonctions de prévention, de contrôle, d'identification, d'assistance, de retour

¹⁴ Conseil de l'Union européenne, *Joint Declaration Establishing a Mobility Partnership between the Kingdom of Morocco and the European Union and its Member States*, doc. 6139/13 ADD 1 REV 3, 3 juin 2013, p. 1-4.

¹⁵ Conseil de l'Union européenne, *Joint Declaration Establishing a Mobility Partnership*, préc., p. 10-11.

ou de lutte contre les réseaux criminels (Carrera *et al.*, 2016: 3-8). La frontière européenne n'est donc pas déplacée mécaniquement au Maroc; elle est prolongée par des instruments de coopération qui agissent en amont du territoire de l'Union.

Les instruments financiers occupent une place centrale dans cette économie juridique. La Commission européenne indique que le Fonds fiduciaire d'urgence de l'Union européenne pour l'Afrique a constitué, entre 2015 et 2021, l'un des principaux outils de financement de l'action migratoire européenne au Maroc, avec environ 234 millions d'euros engagés, principalement pour la gestion intégrée des frontières, la lutte contre le trafic de migrants et la traite des êtres humains, la protection, la stabilisation communautaire, la gouvernance migratoire, la migration de travail et le retour volontaire assisté. Elle précise également qu'un programme de soutien budgétaire de 150 millions d'euros a été alloué en 2022 pour renforcer la coopération UE-Maroc en matière migratoire, tout en appuyant la Stratégie nationale d'immigration et d'asile du Maroc¹⁶. Ces données confirment que la coopération ne se situe pas seulement au niveau discursif: elle repose sur des instruments financiers puissants, orientés vers la capacité administrative, opérationnelle et institutionnelle du partenaire marocain.

La même logique se retrouve dans les documents récents du Conseil de l'Union européenne. Ceux-ci présentent le Maroc comme un partenaire prioritaire de la coopération extérieure en matière migratoire, notamment en raison de son rôle sur les routes de la Méditerranée occidentale et de l'Atlantique. Ils rappellent l'existence d'un portefeuille migratoire important, incluant les financements antérieurs du Fonds fiduciaire d'urgence, le soutien budgétaire adopté dans le cadre de l'instrument NDICI-Global Europe et les programmes régionaux destinés à renforcer la lutte contre les passeurs, la gestion des frontières et le retour volontaire assisté¹⁷. L'économie juridique de la coopération migratoire extérieure de l'Union se présente ainsi comme un assemblage d'instruments financiers et opérationnels qui renforcent progressivement les capacités de contrôle, de surveillance et de gestion des mobilités dans l'espace marocain.

La lutte contre le trafic de migrants et la traite des êtres humains constitue l'un des axes les plus structurants de cette coopération. Le plan d'action de l'Union européenne relatif aux routes de la Méditerranée occidentale et de l'Atlantique mentionne explicitement la mise en œuvre de l'Anti-Smuggling

¹⁶ Commission européenne, *EU Migration Support in Morocco*, février 2023, p. 1.

¹⁷ Conseil de l'Union européenne, *Migration External Cooperation – Action File: Morocco*, 6 février 2024, p. 21-22.

Operational Partnership avec le Maroc. Il prévoit également un soutien aux efforts marocains de lutte contre les réseaux de passeurs et de traite, par l'assistance financière ciblée, le soutien budgétaire, le renforcement des capacités, la coopération avec les États membres et les agences européennes compétentes, ainsi qu'un rapprochement avec Europol et CEPOL¹⁸. Cette évolution montre que le Maroc n'est pas seulement un bénéficiaire de l'assistance européenne; il est intégré à une chaîne opérationnelle de lutte contre les routes migratoires irrégulières et les économies criminelles qui les accompagnent.

La coopération frontalière proprement dite confirme cette analyse. Le même plan d'action prévoit le renforcement de la coopération avec le Maroc en matière de gestion des frontières, notamment par l'usage des financements européens, la fourniture d'équipements, le soutien aux capacités nationales et le développement de la coopération avec Frontex. Les documents du Conseil mentionnent également la feuille de route Frontex-Maroc de 2023 et l'objectif d'approfondir les relations avec les agences de l'Union dans les domaines de la gestion des frontières, de la coopération policière, de l'asile, de la formation et de la lutte contre la criminalité liée aux migrations¹⁹. Il faut toutefois rester juridiquement précis: cette coopération opérationnelle ne signifie pas, en elle-même, que le Maroc serait intégré aux systèmes d'information européens ou qu'il disposerait d'un accès direct aux bases de données de l'Union. Elle indique plutôt l'existence d'une coopération institutionnelle et fonctionnelle autour des objectifs de contrôle, de prévention et d'identification.

Cette précision permet d'éviter une confusion essentielle pour la suite de l'article. La coopération migratoire générale ne doit pas être confondue avec une coopération juridiquement structurée en matière de données personnelles ou biométriques. La première peut prendre la forme d'un dialogue politique, d'un financement, d'une formation, d'un soutien logistique, d'une coopération policière, d'un appui à la gestion des frontières ou d'une coordination contre les réseaux de passeurs. La seconde suppose, en revanche, l'existence de bases légales spécifiques, de finalités déterminées, de garanties relatives à la protection des données, de règles d'accès, de conservation, de traçabilité et de supervision, ainsi que de mécanismes permettant l'exercice effectif des droits des personnes concernées. Autrement dit, le fait que l'Union coopère étroitement avec le Maroc en matière migratoire ne permet pas de présumer

¹⁸ Commission européenne, *EU Action Plan on the Western Mediterranean and Atlantic Routes*, 6 juin 2023, p. 2.

¹⁹ Commission européenne, *EU Action Plan on the Western Mediterranean and Atlantic Routes*, préc., p. 2; Conseil de l'Union européenne, *Migration External Cooperation – Action File: Morocco*, préc., p. 21-22.

l'existence d'un transfert direct ou d'un accès marocain aux systèmes européens tels que l'EES, ETIAS, le VIS, le SIS, Eurodac ou les composants d'interopérabilité²⁰.

Cette distinction est d'autant plus nécessaire que l'externalisation migratoire opère souvent par zones grises. La doctrine relative à la coopération UE-Maroc montre que les instruments employés sont fréquemment hybrides: politiquement engageants sans être pleinement contraignants, financièrement incitatifs sans être formellement conditionnels, opérationnellement denses sans toujours relever d'un traité international spécifique. Carrera, Cassarino, El Qadim, Lahlou et den Hertog soulignent ainsi que le Maroc occupe une place particulière dans la coopération européenne en matière de réadmission, de frontières et de protection: malgré l'ancienneté des négociations relatives à la réadmission, l'Union n'a pas obtenu d'accord complet, notamment en raison de la sensibilité de la clause relative aux ressortissants de pays tiers et des coûts politiques qu'elle ferait peser sur le Maroc (Carrera *et al.*, 2016: 5-8). Cette observation rappelle que l'externalisation n'est pas un processus unilatéral. Le Maroc coopère, mais il négocie également les termes de cette coopération.

La place du Maroc doit donc être appréciée dans une relation à la fois asymétrique et transactionnelle. L'asymétrie tient au poids économique, financier et normatif de l'Union européenne, qui dispose de ressources importantes pour orienter la coopération migratoire. Mais cette asymétrie ne signifie pas passivité du partenaire marocain. Les travaux de Nora El Qadim ont montré que la politique migratoire européenne, vue depuis le Maroc, ne se réduit pas à une imposition extérieure: elle ouvre aussi des marges de négociation, de réinterprétation et de valorisation diplomatique pour l'État partenaire (El Qadim, 2018: 109-112, 121-125). De même, les analyses récentes sur le Fonds fiduciaire d'urgence pour l'Afrique au Maroc insistent sur le caractère réactif, transnational et parfois fragmenté de l'externalisation européenne: loin de former un bloc homogène, l'action européenne se compose d'interventions multiples, auxquelles les autorités marocaines, les États membres et les acteurs internationaux donnent des significations parfois différentes (Gazzotti *et al.*, 2023: 75-79).

La question de la réadmission illustre particulièrement cette économie juridique. L'article 79, paragraphe 3, TFUE permet à l'Union de conclure avec les pays tiers des accords de réadmission pour le retour des ressortissants

²⁰ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, art. 44 à 50; directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, art. 35 à 40; règlement (UE) 2018/1725 du Parlement européen et du Conseil, du 23 octobre 2018, art. 46 à 50.

de pays tiers qui ne remplissent pas ou ne remplissent plus les conditions d'entrée, de présence ou de séjour dans un État membre. Pourtant, dans le cas marocain, les négociations engagées depuis le début des années 2000 n'ont pas abouti à un accord complet. Cette absence d'accord ne signifie pas absence de coopération; elle révèle plutôt le déplacement de la coopération vers d'autres formes: arrangements pratiques, programmes financés, dialogues politiques, mécanismes d'identification, assistance au retour et coopération opérationnelle. Frasca montre que la politique européenne de réadmission tend précisément à s'accompagner de mécanismes de conditionnalité, notamment en matière de visas, lorsque la coopération des pays tiers est jugée insuffisante (Frasca, 2022: 167-170). Dans le cas du Maroc, cette dynamique doit être lue avec prudence: elle ne traduit pas une intégration juridique complète, mais une pression continue pour articuler mobilité, retour, visas et coopération sécuritaire.

Il en résulte que le Maroc occupe une place stratégique dans l'économie juridique de la coopération migratoire extérieure de l'Union. Cette place tient à la combinaison d'un positionnement géographique sensible, d'une coopération politique ancienne, d'un financement européen substantiel, d'une implication opérationnelle croissante et d'une capacité de négociation propre. Le Maroc apparaît ainsi comme un partenaire à la fois sollicité, financé, responsabilisé et capable d'infléchir les termes de la coopération, ce qui empêche de réduire la relation UE-Maroc à une simple sous-traitance du contrôle migratoire européen.

Cette centralité doit toutefois être juridiquement qualifiée. Le Maroc est central dans la projection externe de la gouvernance migratoire européenne; il ne l'est pas nécessairement dans l'architecture interne des systèmes européens d'information. La coopération UE-Maroc crée un environnement favorable à l'échange d'informations, à l'identification des personnes, à la vérification documentaire, à la lutte contre les réseaux et à l'organisation des retours. Mais la circulation des données biométriques ne peut être présumée à partir de la seule densité de la coopération migratoire générale. Elle doit être analysée mécanisme par mécanisme: transfert direct, accès indirect, assistance technique, communication ponctuelle, résultat d'identification ou externalisation fonctionnelle (Carrera, 2016).

2. LES FORMES POSSIBLES DE CIRCULATION DES DONNÉES BIOMÉTRIQUES: TRANSFERT, ACCÈS INDIRECT ET EXTERNALISATION FONCTIONNELLE

Après avoir établi que le Maroc occupe une place centrale dans la projection externe de la gouvernance migratoire européenne, il faut éviter une

déduction trop rapide: la densité de la coopération migratoire UE-Maroc ne signifie pas, par elle-même, que les autorités marocaines auraient accès aux systèmes européens d'information, ni qu'il existerait un flux direct et généralisé de données biométriques entre l'Union et le Maroc. C'est précisément ici que se situe l'enjeu juridique principal. La coopération migratoire extérieure crée un environnement favorable à l'échange d'informations, à l'identification des personnes, à la vérification documentaire, à la lutte contre les réseaux de passeurs et à l'organisation des retours; mais elle ne produit pas automatiquement un régime de circulation biométrique. Il convient donc de distinguer plusieurs figures juridiquement différentes: le transfert direct de données, l'accès indirect ou médié, l'échange informationnel sans transfert intégral, l'assistance technique à l'identification et, enfin, l'externalisation fonctionnelle du contrôle.

Dans le cas marocain, ces figures ne doivent pas être comprises comme des hypothèses purement abstraites. Elles trouvent des points d'ancrage dans plusieurs instruments opérationnels déjà identifiables de la coopération UE-Maroc. Les documents européens relatifs à la coopération extérieure en matière migratoire mentionnent le Maroc comme un partenaire important sur les routes de la Méditerranée occidentale et de l'Atlantique; les financements du Fonds fiduciaire d'urgence de l'Union européenne pour l'Afrique, puis les programmes relevant du NDICI-Global Europe, ont soutenu la gestion intégrée des frontières, la lutte contre le trafic de migrants, la protection, la gouvernance migratoire et les retours volontaires assistés; le plan d'action de l'Union pour les routes occidentale méditerranéenne et atlantique évoque également le renforcement de la coopération avec les agences européennes, notamment dans la lutte contre les réseaux de passeurs. Ces instruments ne permettent pas d'affirmer l'existence d'un transfert biométrique généralisé vers le Maroc, mais ils permettent d'identifier les séquences dans lesquelles une circulation informationnelle peut juridiquement apparaître: confirmation d'identité, vérification documentaire, appui consulaire à l'identification, délivrance de documents de voyage, préparation des retours, coopération opérationnelle ou transmission limitée d'un résultat d'identification.

La première figure est celle du transfert direct de données personnelles, éventuellement biométriques, vers un pays tiers. En droit de l'Union, un tel transfert ne peut pas être assimilé à une simple coopération administrative. Il suppose qu'un responsable du traitement ou un sous-traitant soumis au droit de l'Union transmette ou rende disponibles des données personnelles à un destinataire distinct situé dans un pays tiers ou relevant d'une organisation internationale. Le Comité européen de protection des données (CEPD) précise que la notion de transfert doit être appréciée à partir de trois critères cumulatifs: l'exportateur doit être soumis au RGPD, il doit transmettre ou

rendre accessibles des données personnelles à un autre responsable, responsable conjoint ou sous-traitant, et cet importateur doit se situer dans un pays tiers ou au sein d'une organisation internationale²¹. Cette définition est essentielle pour le sujet traité: si des données biométriques issues d'un système européen étaient communiquées à une autorité marocaine, ou rendues accessibles à celle-ci, l'opération ne relèverait pas d'un simple échange opérationnel; elle devrait être qualifiée de transfert international soumis aux exigences du droit de l'Union (Kuner, 2013).

Ce régime est d'autant plus exigeant que les données biométriques présentent une intensité particulière. Elles ne constituent pas de simples données d'identité; elles rattachent l'identification administrative au corps de la personne. Le transfert de telles données vers un État tiers doit donc respecter non seulement les conditions générales des transferts internationaux, mais également les exigences relatives aux catégories particulières de données, à la finalité du traitement, à la nécessité, à la proportionnalité, à la minimisation et à la sécurité. En outre, lorsqu'une autorité d'un pays tiers sollicite directement la communication de données, la demande étrangère ne constitue pas en elle-même une base juridique suffisante. Le CEPD rappelle, à propos de l'article 48 du RGPD, qu'une décision ou demande d'une autorité d'un pays tiers ne peut produire effet dans l'Union que dans les conditions prévues par un accord international ou par les mécanismes applicables du chapitre V du RGPD²². Il en résulte qu'un transfert biométrique vers le Maroc ne saurait être déduit de la seule existence d'une coopération migratoire ou policière: il devrait reposer sur une base juridique identifiable et sur des garanties effectives. Cette exigence rejoint la logique de l'avis 1/15 de la Cour de justice, selon laquelle la communication de données personnelles à un pays tiers constitue une ingérence dans les droits garantis par les articles 7 et 8 de la Charte et doit, pour cette raison, être entourée de règles claires, précises et accessibles concernant les finalités du traitement, les catégories de données transférées, les destinataires, la durée de conservation, le contrôle indépendant et les voies de recours²³.

À ce jour, le Maroc ne bénéficie pas d'une décision d'adéquation de la Commission européenne au titre de l'article 45 du RGPD. Cette absence ne

²¹ CEPD, *Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux du chapitre V du RGPD*, version 2.0, adoptées le 14 février 2023, p. 3 et 6-8.

²² Règlement (UE) 2016/679, art. 44 à 50; directive (UE) 2016/680, art. 35 à 40; règlement (UE) 2018/1725, art. 46 à 50; CEPD, *Guidelines 02/2024 on Article 48 GDPR*, version 2.1, adoptées le 4 juin 2025, p. 3 et 7-8.

²³ CJUE, avis 1/15, Accord PNR entre le Canada et l'Union européenne, 26 juillet 2017, ECLI:EU:C:2017:592, points 124-141 et 163-174.

signifie pas que tout transfert serait absolument impossible, mais elle interdit de considérer le Maroc comme un espace juridiquement équivalent à l'Union en matière de protection des données. En l'absence d'adéquation, la circulation de données personnelles vers le Maroc doit donc être fondée sur des garanties appropriées, des instruments spécifiques ou, de manière exceptionnelle, sur des dérogations encadrées. L'arrêt *Schrems II* confirme, à cet égard, que l'absence de décision d'adéquation impose d'apprécier concrètement si les garanties mobilisées assurent un niveau de protection substantiellement équivalent à celui garanti dans l'Union, compte tenu non seulement des clauses ou instruments utilisés, mais aussi du droit et des pratiques du pays tiers ainsi que de l'existence de mécanismes effectifs de contrôle et de recours²⁴. Francesca Tassinari souligne, dans une étude consacrée à l'externalisation du droit européen de la protection des données au Maroc, que l'échange de données entre l'Union et le Maroc demeure juridiquement contraint par l'absence d'un niveau de protection reconnu comme équivalent au standard européen (Tassinari, 2021: 5-6, 8-9). Cette situation impose de distinguer la coopération migratoire générale, qui peut être large, de la coopération en matière de données, qui demeure juridiquement conditionnée²⁵.

Le droit de l'Union connaît néanmoins des hypothèses limitées de communication de données à des pays tiers dans le cadre du retour. Le règlement relatif à l'utilisation du système d'information Schengen aux fins du retour prévoit, dans des conditions strictes, la possibilité de transférer certaines données personnelles à un pays tiers pour identifier un ressortissant de pays tiers en séjour irrégulier et obtenir un document de voyage en vue de son retour. Le document de travail de la Commission relatif aux menaces sécuritaires et au retour rappelle que cette communication peut porter notamment sur des données d'identité, des photographies, des données dactyloscopiques et des copies de documents d'identité, mais uniquement pour l'identification et la délivrance d'un document de voyage, avec l'accord de l'État membre ayant introduit le signalement et l'information de la personne concernée²⁶. Il ne s'agit donc pas d'un accès général du pays tiers au SIS, mais d'une communication ciblée, finalisée et conditionnée.

²⁴ CJUE, grande chambre, 16 juillet 2020, Data Protection Commissioner c. Facebook Ireland Ltd et Maximilian Schrems, C-311/18, EU:C:2020:559, points 92-96, 101-107 et 129-134.

²⁵ Commission européenne, «Data protection adequacy for non-EU countries», rubrique consacrée aux décisions d'adéquation au titre de l'article 45 du RGPD.

²⁶ 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, art.

Une logique comparable apparaît dans le nouveau règlement Eurodac de 2024. Celui-ci étend les finalités du système, notamment en matière d'identification des ressortissants de pays tiers en séjour irrégulier et de soutien aux politiques de retour. Il maintient toutefois le principe selon lequel les données issues d'Eurodac ne peuvent pas être librement transférées à des pays tiers. La possibilité de communication à un pays tiers demeure conçue comme une dérogation strictement encadrée, destinée à assister l'identification d'une personne en vue du retour, et non comme un mécanisme d'accès externe au système européen²⁷. Cette distinction est capitale pour l'analyse UE-Maroc: même lorsque le droit européen prévoit une communication vers un pays tiers, celle-ci ne transforme pas l'État tiers en utilisateur du système européen. Elle l'insère seulement, de manière ponctuelle, dans une chaîne d'identification ou de ré-documentation.

La deuxième figure est celle de l'accès indirect ou médié. Elle se distingue du transfert direct en ce que l'autorité du pays tiers ne reçoit pas nécessairement les données brutes, ni l'accès technique à la base européenne. Elle peut recevoir le résultat d'une vérification, une confirmation d'identité, une demande de reconnaissance consulaire, une information nécessaire à la délivrance d'un laissez-passer ou un élément limité permettant d'établir la nationalité ou l'identité de la personne. Dans ce modèle, la consultation du système reste effectuée par une autorité européenne habilitée, mais le résultat de cette consultation peut être utilisé dans une procédure impliquant un État tiers. Juridiquement, la difficulté tient à ce que l'accès au résultat peut parfois produire les mêmes effets pratiques qu'un accès à la donnée, tout en étant moins visible et moins formalisé.

Cette forme d'accès médié correspond à une zone grise classique de la coopération migratoire. D'un côté, elle ne peut être assimilée à un accès direct aux systèmes européens; de l'autre, elle peut participer à la circulation fonctionnelle d'informations personnelles. L'enjeu consiste donc à déterminer si le pays tiers reçoit une donnée personnelle identifiable, un simple résultat opérationnel ou une information suffisamment individualisée pour être qualifiée de donnée personnelle. Le CEPD considère que le fait de rendre des données accessibles, y compris par un accès à distance ou par l'attribution de droits d'accès, peut constituer un transfert international lorsque les critères du

15; Commission européenne, *Commission Staff Working Document on Enhancing Cooperation on Security Threats and Return*, SWD(2024) 287 final, 16 décembre 2024, p. 8.

²⁷ Règlement (UE) 2024/1358 du Parlement européen et du Conseil, du 14 mai 2024, relatif à la création d'Eurodac pour la comparaison des données biométriques, considérant 67 et art. 49-50.

chapitre V sont réunis²⁸. Cela signifie que, si une autorité marocaine disposait d'un accès technique, même limité ou distant, à des données européennes, l'opération devrait être qualifiée juridiquement et soumise au régime des transferts. En revanche, lorsque seule une autorité européenne interroge le système et communique ensuite un résultat limité, l'analyse doit porter sur la nature exacte de l'information communiquée.

La troisième figure est celle de l'échange informationnel sans transfert intégral. Elle vise les hypothèses dans lesquelles les autorités coopèrent autour d'une identité, d'une nationalité, d'un document ou d'une procédure de retour sans que la base de données européenne elle-même soit transférée ou ouverte. Cette coopération peut prendre la forme d'une demande d'identification adressée à une autorité consulaire, de la transmission d'éléments biographiques, de la communication d'une photographie, d'une comparaison documentaire, d'un échange sur l'authenticité d'un document ou d'une demande de délivrance d'un laissez-passer. La donnée biométrique peut y intervenir de manière ponctuelle, mais elle n'est pas nécessairement transférée sous forme brute ou massive.

La pratique européenne montre que ces échanges sont fréquents dans les politiques d'identification et de retour. Le Réseau européen des migrations relève que plusieurs États membres autorisent, dans certaines conditions, le transfert international de données biométriques, notamment pour faciliter le retour ou l'éloignement, mais que ces transferts sont généralement limités à des situations particulières et encadrés par la loi, un traité ou un instrument européen²⁹. Cette observation confirme que la circulation biométrique n'est pas un phénomène uniforme. Elle peut aller d'une communication individualisée à un transfert plus structuré, mais elle ne peut être comprise sans examiner le fondement juridique, la finalité, le destinataire, la nature des données et le degré d'accès accordé.

La quatrième figure est celle de l'assistance technique à l'identification. Elle ne consiste pas nécessairement en un transfert de données européennes vers le Maroc. Elle peut prendre la forme d'un financement d'équipements, d'une formation des autorités nationales, d'un appui à la gestion intégrée des frontières, d'un soutien à la détection documentaire, d'un renforcement des capacités d'enregistrement ou de dispositifs de coopération avec des agences européennes. Luisa Marin montre que la coopération de Frontex avec les pays tiers ne se limite pas aux opérations visibles: elle comprend également des arrangements de travail, des échanges d'informations, des réseaux d'analyse du risque, des officiers de liaison et des formes d'assistance technique qui

²⁸ CEPD, *Lignes directrices 05/2021*, préc., p. 7-8.

²⁹ European Migration Network, *Processing the Biometric Data of Third-Country Nationals*, EMN Inform, 10 décembre 2024, p. 3-4.

structurent la gestion externe des frontières (Marin, 2020: 157-163, 168-170). Ces instruments ne créent pas nécessairement un transfert de données, mais ils peuvent rendre les systèmes administratifs plus compatibles, plus inter-connectables ou plus orientés vers les standards européens d'identification.

Dans le cas marocain, cette assistance doit être analysée avec prudence. Elle peut contribuer à moderniser les capacités nationales de gestion des frontières, à améliorer la lutte contre le trafic de migrants ou à renforcer l'identification documentaire. Mais elle peut aussi produire une convergence fonctionnelle entre les pratiques marocaines et les attentes européennes. Tassinari souligne que l'externalisation européenne ne passe pas seulement par le transfert de normes juridiques, mais également par des dispositifs opérationnels et techniques liés à la gestion des flux migratoires et à la coopération en matière de retour (Tassinari, 2021: 15-17). L'assistance technique devient ainsi une forme indirecte de circulation de la rationalité biométrique: même sans accès marocain aux systèmes européens, les pratiques nationales peuvent être orientées vers des méthodes d'identification compatibles avec les besoins européens de contrôle, de retour ou de réadmission.

La cinquième figure est celle de l'externalisation fonctionnelle du contrôle. Elle désigne une situation dans laquelle un État tiers participe de fait à une chaîne européenne de vérification, d'identification, de prévention ou de retour, sans être juridiquement intégré à l'architecture interne des bases de données de l'Union. C'est ici que l'analyse doit être la plus fine. Le Maroc peut participer à la surveillance des routes migratoires, à la lutte contre les réseaux, à la prévention des départs, à l'identification de personnes, à la coopération consulaire et au retour, sans pour autant disposer d'un accès direct à l'EES, à ETIAS, au VIS, au SIS, à Eurodac ou aux composants d'interopérabilité. L'externalisation fonctionnelle ne suppose donc pas l'intégration informatique; elle suppose une participation opérationnelle à une chaîne de contrôle.

Cette distinction permet de dépasser une lecture trop binaire. D'un côté, il serait juridiquement inexact d'affirmer que la coopération UE-Maroc implique automatiquement un partage biométrique direct ou un accès marocain aux systèmes européens. De l'autre, il serait insuffisant de soutenir que l'absence d'accès direct exclut toute circulation informationnelle. Entre l'accès intégral et l'absence totale d'échange, il existe une pluralité de mécanismes intermédiaires: transmission ciblée, confirmation d'identité, résultat d'une comparaison, demande consulaire, assistance à la ré-documentation, appui technique, formation, financement d'outils d'identification ou coopération opérationnelle dans la lutte contre les réseaux. C'est dans ces mécanismes intermédiaires que se logent les principaux enjeux juridiques.

Le risque de glissement des finalités apparaît ici de manière particulière. Une donnée collectée dans un contexte de visa, d'asile, de franchissement de frontière ou de séjour peut être ultérieurement mobilisée pour l'identification

d'une personne en retour, pour la lutte contre l'immigration irrégulière ou pour une coopération avec un pays tiers. La difficulté ne réside pas seulement dans le transfert matériel de la donnée, mais dans la réorientation de sa finalité. Marin souligne que les pratiques de coopération informationnelle avec les pays tiers brouillent les frontières entre contrôle migratoire, gestion des frontières, coopération policière, sécurité intérieure et lutte contre la criminalité (Marin, 2020: 172-175). Dans un environnement interopérable, ce brouillage peut être renforcé, car une même information peut devenir utile dans plusieurs chaînes décisionnelles.

La question des chaînes de responsabilité est également centrale. Lorsque plusieurs acteurs interviennent — État membre, agence européenne, autorité consulaire d'un pays tiers, autorité administrative nationale, prestataire technique ou organisation internationale — il devient plus difficile d'identifier le responsable exact d'un traitement, l'autorité compétente pour rectifier une erreur, le juge compétent pour contrôler la légalité de l'usage de la donnée et le mécanisme disponible pour exercer un recours effectif. L'externalisation fonctionnelle produit ainsi un risque de dilution: la décision peut être prise dans un État membre, préparée par une donnée issue d'un système européen, facilitée par une coopération avec un pays tiers et exécutée par une procédure de retour ou de réadmission. La personne concernée peut alors se trouver confrontée à une chaîne décisionnelle transnationale dont les points de contestation sont fragmentés.

Cette difficulté est particulièrement sensible en matière biométrique. Si une erreur affecte une empreinte, une image faciale, une identité consolidée ou une correspondance entre plusieurs systèmes, ses effets peuvent se propager dans différentes procédures. Une identité mal associée peut orienter une demande de réadmission; une correspondance biométrique peut faciliter la délivrance d'un document de voyage; une information communiquée à une autorité consulaire peut contribuer à établir une nationalité; un résultat de vérification peut produire des effets dans une procédure d'éloignement. La circulation biométrique doit donc être appréciée non seulement à partir de la question «qui accède à la donnée ?», mais aussi à partir de la question «quels effets juridiques produit le résultat de cette donnée ?».

Cette approche permet de mieux situer le cas UE-Maroc. La coopération migratoire euro-marocaine peut produire des effets informationnels sans nécessairement organiser un transfert direct et généralisé de données biométriques. Le Maroc peut être associé à des procédures d'identification, de prévention, de retour ou de lutte contre le trafic de migrants, tout en demeurant extérieur aux bases européennes. Inversement, certaines communications individualisées de données peuvent être juridiquement possibles, mais seulement si elles respectent les conditions prévues par les instruments européens applicables, notamment en matière de retour, de protection des données et de finalité. La coopération doit

donc être pensée à partir d'une échelle d'intensité: absence de données personnelles, échange d'informations non biométriques, communication ciblée de données d'identité, transmission ponctuelle de données biométriques, accès médié à un résultat, transfert juridiquement qualifié, ou accès technique direct — cette dernière hypothèse étant la plus exigeante et ne pouvant être présumée.

L'apport doctrinal de cette cartographie est de montrer que la circulation des données biométriques ne constitue pas un bloc homogène. Elle peut prendre des formes juridiquement très différentes, qui n'appellent pas le même régime de validité. Le transfert direct suppose l'application des règles sur les transferts internationaux. L'accès indirect appelle une analyse de la mise à disposition et de la nature du résultat communiqué. L'échange informationnel sans transfert intégral doit être apprécié au regard de la qualification de donnée personnelle et de la finalité poursuivie. L'assistance technique soulève la question de la convergence opérationnelle et de la diffusion des standards européens d'identification. L'externalisation fonctionnelle, enfin, oblige à examiner les effets pratiques de la coopération, même en l'absence d'intégration formelle du pays tiers aux bases de données de l'Union.

Il en résulte que la coopération UE-Maroc ne doit pas être lue comme une alternative simple entre accès et nonaccès. Elle doit être analysée comme un continuum de mécanismes informationnels, dont certains sont pleinement juridiques, d'autres opérationnels, d'autres encore situés dans des zones grises. Cette approche est indispensable pour éviter deux erreurs inverses: surestimer la coopération en affirmant sans preuve l'existence d'un accès marocain aux systèmes européens; ou la sous-estimer en considérant que l'absence d'un tel accès exclurait toute forme de circulation biométrique ou d'externalisation informationnelle.

La conclusion de cette sous-partie est donc la suivante: la circulation des données biométriques dans la coopération UE-Maroc ne doit pas être pensée comme un phénomène unique, mais comme une pluralité de mécanismes juridiquement distincts. Ce n'est qu'en distinguant le transfert, l'accès médié, la communication ponctuelle, l'assistance technique et l'externalisation fonctionnelle que l'on peut apprécier correctement les risques pesant sur la vie privée, la protection des données personnelles et le recours effectif. Cette cartographie prépare ainsi le test de validité juridique qui devra être conduit dans la sous-partie suivante: les garanties fondamentales ne pourront pas être appliquées de manière abstraite; elles devront être ajustées à chaque forme de circulation, selon son intensité, sa finalité, son destinataire et ses effets sur la personne concernée.

Afin de clarifier la délimitation entre ces différentes figures, il est possible de les distinguer à partir de cinq critères: la base juridique mobilisable, la nature de l'information transmise, l'autorité responsable du traitement, les garanties exigibles et la voie de recours ouverte à la personne concernée.

TABLEAU 1. *Typologie juridique des formes de circulation informationnelle et des garanties applicables dans la coopération UE-Maroc.*

<i>Figure typologique</i>	<i>Base juridique mobilisable</i>	<i>Nature de l'information transmise</i>	<i>Responsable du traitement</i>	<i>Garanties exigibles</i>	<i>Voie de recours</i>
Transfert direct de données	RGPD, règlement 2018/1725, directive 2016/680, accord international ou garanties appropriées	Données personnelles individualisées, éventuellement biométriques	Autorité exportatrice et destinataire situé dans l'État tiers	Base légale, finalité déterminée, minimisation, sécurité, traçabilité, contrôle indépendant	Droit d'accès, rectification, effacement, recours devant l'autorité de contrôle ou le juge compétent
Accès médié	Droit dérivé applicable au système concerné et règles d'habilitation des autorités européennes ou nationales	Résultat obtenu par une autorité européenne ou nationale après consultation d'un système européen	Autorité ayant interrogé le système et communiqué le résultat	Absence d'accès direct de l'État tiers, journalisation, limitation de la finalité, contrôle des habilitations	Contestation de la décision individuelle fondée sur le résultat communiqué
Communication ponctuelle	Base légale spécifique liée à l'identification, au retour, à la réadmission ou à la délivrance d'un document de voyage	Éléments limités d'identité, photographie, empreintes, copie de document ou confirmation d'identité	Autorité qui communique l'information au cas par cas	Nécessité concrète, proportionnalité, information de la personne lorsque possible, limitation de conservation	Recours contre la décision de retour, de réadmission ou contre le traitement des données

<i>Figure typologique</i>	<i>Base juridique mobilisable</i>	<i>Nature de l'information transmise</i>	<i>Responsable du traitement</i>	<i>Garanties exigibles</i>	<i>Voie de recours</i>
Échange d'informations sans transfert intégral	Coopération opérationnelle ou policière encadrée par une finalité déterminée	Indice, concordance, confirmation, information ou résultat d'identification sans transmission complète du fichier	Autorité qui produit et transmet le résultat informationnel	Qualification du résultat comme donnée personnelle lorsqu'il permet d'identifier une personne, traçabilité, limitation stricte de la finalité	Droit d'accès direct ou indirect, contrôle par une autorité indépendante, contestation de la décision fondée sur l'information
Assistance technique et externalisation fonctionnelle	Programmes financiers, coopération opérationnelle, instruments de renforcement capacitaire	Pas nécessairement de donnée transmise, diffusion de standards, outils, méthodes ou capacités d'identification	Autorités bénéficiaires et, selon les cas, institutions ou agences finançant ou encadrant le dispositif	Évaluation des risques, conditionnalité des droits fondamentaux, audits, supervision, prévention des usages détournés	Recours contre les décisions nationales produisant des effets individuels et contrôle de la responsabilité institutionnelle

Source: *Élaboration de l'auteur.*

Cette distinction permet d'éviter deux confusions. D'une part, l'absence d'accès direct du Maroc aux systèmes européens ne suffit pas à exclure toute circulation informationnelle juridiquement pertinente. D'autre part, toute coopération opérationnelle ne constitue pas nécessairement un transfert international de données. L'enjeu consiste donc à qualifier chaque mécanisme selon ses effets réels sur l'identification, la décision administrative et les droits de la personne concernée.

3. LES GARANTIES FONDAMENTALES COMME LIMITE ET CONDITION DE VALIDITÉ DE LA COOPÉRATION BIOMÉTRIQUE

La cartographie précédente a permis de montrer que la circulation des données biométriques dans la coopération UE-Maroc ne doit pas être pensée comme un phénomène unique. Elle peut prendre la forme d'un transfert direct, d'un accès indirect, d'une communication ponctuelle, d'une assistance technique à l'identification ou d'une externalisation fonctionnelle du contrôle. Cette pluralité de mécanismes appelle désormais un test de validité juridique. En effet, plus la coopération migratoire se rapproche d'une coopération informationnelle, plus elle doit être appréciée au regard des garanties fondamentales qui encadrent le traitement des données personnelles, en particulier lorsqu'il s'agit de données biométriques. Ces garanties ne constituent donc pas un supplément éthique ajouté à une coopération déjà licite; elles déterminent les conditions mêmes de sa licéité.

Le point de départ doit être la Charte des droits fondamentaux de l'Union européenne. Les articles 7 et 8 protègent respectivement le droit au respect de la vie privée et familiale et le droit à la protection des données personnelles. L'article 47 garantit le droit à un recours effectif et à accéder à un tribunal impartial. L'article 52, paragraphe 1, fixe le régime général des limitations aux droits garantis par la Charte: toute limitation doit être prévue par la loi, respecter le contenu essentiel des droits, répondre effectivement à un objectif d'intérêt général reconnu par l'Union ou au besoin de protéger les droits et libertés d'autrui, et satisfaire aux exigences de nécessité et de proportionnalité (Lenaerts, 2019: 779-781, 791-793)³⁰. Cette architecture impose une conséquence immédiate: une coopération biométrique ne peut être juridiquement admise que si elle repose sur une base légale claire, poursuit des finalités déterminées, limite strictement les données traitées et demeure contrôlable par des autorités indépendantes et par le juge (Lynskey, 2015).

³⁰ Charte des droits fondamentaux de l'Union européenne, art. 7, 8, 47 et 52, JOUE C 326, 26 octobre 2012.

Cette exigence de base légale claire est première. La biométrie ne peut être encadrée par des formules générales renvoyant abstraitement à la gestion migratoire, à la sécurité des frontières ou à la coopération avec les pays tiers. Le traitement de données biométriques constitue une ingérence sérieuse dans les droits garantis par les articles 7 et 8 de la Charte, car ces données permettent ou confirment l'identification unique d'une personne à partir de caractéristiques physiques, physiologiques ou comportementales. Le CEPD rappelle, à propos de la reconnaissance faciale dans le champ répressif, que le traitement biométrique soulève directement la question du respect de la vie privée et de la protection des données, et qu'il suppose une base légale suffisamment précise quant aux objectifs, aux catégories de données, aux finalités et aux garanties applicables³¹. Transposée à la coopération UE-Maroc, cette exigence signifie qu'il ne suffit pas d'invoquer la coopération migratoire ou la lutte contre l'immigration irrégulière: il faut identifier l'instrument juridique qui autorise le traitement, les autorités compétentes, les catégories de données concernées, les destinataires, les conditions d'accès et les droits de la personne.

La finalité déterminée constitue la deuxième garantie structurante. Les données biométriques ne peuvent être collectées ou communiquées pour une finalité indéfinie de «bonne gestion des migrations». Une donnée recueillie pour contrôler un franchissement de frontière ne peut être réutilisée sans limite pour l'éloignement, la coopération policière, la lutte contre le trafic de migrants ou la vérification consulaire. Toute extension de finalité doit être juridiquement justifiée. C'est ici que le risque de glissement de finalité devient central. La coopération biométrique avec un pays tiers peut déplacer la donnée hors du contexte initial de collecte et l'insérer dans une autre chaîne décisionnelle: identification, retour, réadmission, délivrance d'un document de voyage ou coopération sécuritaire. La finalité doit donc être énoncée avec précision: identification d'une personne déterminée, vérification documentaire, prévention d'une fraude d'identité, exécution d'une décision de retour ou délivrance d'un laissez-passer consulaire. À défaut, la coopération biométrique risque de devenir une infrastructure générale de disponibilité des corps, ce qui serait incompatible avec l'exigence de limitation des finalités.

La nécessité et la proportionnalité forment le troisième niveau du contrôle. Même lorsqu'une finalité légitime existe, le traitement biométrique ne peut être admis que s'il est nécessaire pour atteindre cette finalité et proportionné à l'intensité de l'atteinte portée aux droits fondamentaux. Le Contrôleur européen de la protection des données a rappelé, dans son avis de 2025 sur le

³¹ CEPD, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, version 2.0, adoptées le 26 avril 2023, p. 13-14 et 19-20.

système commun de retour, que l'efficacité des politiques de migration et d'asile ne dispense pas l'Union de respecter les droits à la vie privée et à la protection des données; il recommande même une analyse approfondie d'impact sur les droits fondamentaux lorsque les mesures envisagées sont susceptibles d'affecter significativement les personnes concernées³². Dans le cadre UE-Maroc, cette exigence implique qu'avant tout transfert ou toute communication biométrique, l'autorité compétente doit démontrer qu'un moyen moins intrusif ne permettrait pas d'atteindre le même résultat: échange de données biographiques, vérification documentaire, entretien consulaire, coopération administrative non biométrique ou transmission limitée d'un résultat sans communication de la donnée brute.

La minimisation des données découle directement de cette exigence. Une coopération biométrique juridiquement admissible ne doit pas transmettre plus de données que ce qui est strictement requis. Si une photographie suffit à établir l'identité, la transmission d'empreintes digitales peut être excessive. Si une confirmation d'identité suffit, la communication intégrale d'un gabarit biométrique peut être disproportionnée. Si l'objectif est la délivrance d'un laissez-passer, les données relatives à une procédure d'asile, à une vulnérabilité médicale ou à une situation familiale ne doivent pas être communiquées, sauf nécessité rigoureusement établie. La minimisation n'est donc pas une règle technique; elle est une garantie substantielle contre la transformation de la coopération migratoire en circulation indifférenciée d'informations personnelles.

La durée de conservation constitue un autre critère décisif. La donnée biométrique est particulièrement sensible parce qu'elle ne peut pas être facilement modifiée par la personne concernée. Une erreur sur une adresse peut être corrigée; une empreinte ou une image faciale, une fois compromises ou indûment associées à une identité, peuvent produire des effets persistants. La durée de conservation doit donc être déterminée par la finalité concrète du traitement. Les systèmes européens eux-mêmes prévoient des délais spécifiques: dans le cadre de l'EES, les données sont conservées selon des durées prévues par le règlement, notamment pour permettre la vérification des entrées, sorties et refus d'entrée, tandis que les droits à l'information, d'accès, de rectification, d'effacement et de recours sont explicitement organisés (Wojnowska-Radzińska, 2019: 113-119)³³. Dans une coopération avec un

³² Contrôleur européen de la protection des données, *Opinion 9/2025 on the Proposal for a Regulation Establishing a Common System for the Return of Third-Country Nationals Staying Illegally in the Union*, 23 mai 2025, p. 2 et 5.

³³ Règlement (UE) 2017/2226 du Parlement européen et du Conseil, du 30 novembre 2017, portant création d'un système d'entrée/de sortie, art. 34, 50 et 52.

pays tiers, cette exigence doit être redoublée: la transmission d'une donnée ne doit pas conduire à une conservation illimitée dans un système externe, ni à une réutilisation ultérieure pour des finalités non prévues.

La traçabilité des accès est également indispensable. Plus la coopération est indirecte, plus il devient difficile pour la personne concernée de savoir quelle autorité a consulté, transmis ou utilisé ses données. Or, sans journalisation des accès, il n'existe pas de contrôle effectif. La traçabilité doit permettre d'identifier l'autorité qui a accédé à la donnée, la date de l'accès, la finalité poursuivie, la base légale mobilisée, les données consultées ou communiquées, ainsi que le destinataire éventuel. Cette garantie est particulièrement importante dans les hypothèses d'accès médié ou d'externalisation fonctionnelle, où l'État tiers ne reçoit pas nécessairement un accès direct à la base européenne, mais peut recevoir un résultat d'identification ou une information individualisée. Dans ces cas, il ne suffit pas de sécuriser la base de données; il faut sécuriser la chaîne décisionnelle.

La supervision indépendante constitue ensuite une condition de crédibilité de l'ensemble du dispositif. Les garanties ne peuvent être abandonnées aux seules autorités opérationnelles chargées du contrôle migratoire. Les autorités de protection des données, les mécanismes de supervision coordonnée des systèmes européens, le Contrôleur européen de la protection des données — European Data Protection Supervisor, EDPS — et les autorités nationales compétentes doivent pouvoir contrôler les traitements, les transferts, les accès et les éventuelles restrictions aux droits des personnes. Le CEPD rappelle que les restrictions aux droits des personnes concernées doivent être encadrées par une mesure législative précise, passer un test de nécessité et de proportionnalité, identifier les responsables du traitement, prévoir les durées de conservation et évaluer les risques pour les personnes concernées, notamment les groupes vulnérables³⁴. Dans le cadre de la coopération UE-Maroc, cela implique que les arrangements opérationnels, même lorsqu'ils ne prennent pas la forme d'un accord international classique, ne doivent pas échapper à l'exigence de contrôle indépendant.

Le droit à l'information constitue une autre garantie fondamentale. La personne concernée doit pouvoir comprendre quelles données sont collectées, pourquoi elles le sont, pendant combien de temps elles seront conservées, qui peut y accéder, si elles peuvent être transmises à un pays tiers et quels droits peuvent être exercés. Cette exigence est particulièrement importante dans les procédures de retour, car les données utilisées peuvent contribuer à fonder une décision défavorable. L'EDPS insiste sur le fait que l'information relative aux motifs de fait d'une

³⁴ CEPD, *Guidelines 10/2020 on Restrictions under Article 23 GDPR*, version 2.1, adoptées le 13 octobre 2021, p. 13-16.

décision de retour soutient l'exercice du recours effectif et que toute limitation de cette information doit rester exceptionnelle, strictement nécessaire et compatible avec les exigences du RGPD³⁵. Il en résulte qu'une coopération biométrique ne peut pas fonctionner dans l'opacité: même lorsque certaines informations peuvent être limitées pour des raisons légitimes de sécurité, la personne doit au minimum disposer d'une information suffisante pour comprendre l'essence des motifs de la décision et exercer utilement ses droits.

Le droit d'accès, de rectification et d'effacement est la condition pratique du contrôle individuel. Dans une architecture biométrique, l'erreur peut avoir des conséquences lourdes: fausse correspondance, identité multiple apparente, confusion entre deux personnes, rattachement erroné à une nationalité, obstacle à l'entrée, éloignement ou réadmission. Le droit d'accès permet à la personne de savoir quelles données sont traitées; le droit de rectification permet de corriger les erreurs; le droit à l'effacement permet d'obtenir la suppression des données conservées illégalement ou devenues inutiles. Le CEPD souligne que le droit d'accès vise précisément à permettre aux personnes de contrôler leurs données, de comprendre le traitement et d'en vérifier la licéité³⁶. Dans une coopération externalisée, ces droits doivent rester effectifs même lorsque plusieurs autorités interviennent. La personne ne doit pas être renvoyée d'une autorité à l'autre sans pouvoir identifier le responsable du traitement ni obtenir une réponse utile.

Le recours effectif est enfin la garantie qui donne une portée juridictionnelle aux droits précédents. Sans recours, la protection des données reste déclaratoire. L'article 47 de la Charte impose que la personne puisse contester une décision défavorable fondée, directement ou indirectement, sur un traitement biométrique. Cette exigence doit être lue à la lumière de l'arrêt *Ligue des droits humains*, dans lequel la Cour de justice a rappelé que les traitements de données poursuivant des finalités de prévention, de détection ou de poursuite d'infractions doivent être strictement encadrés par les principes de nécessité, de proportionnalité, de limitation des finalités et par un contrôle effectif, en particulier lorsqu'ils peuvent conduire à des effets individualisés défavorables³⁷. Elle doit également être rapprochée de l'arrêt *Boudjlida*, où la Cour rattache le droit d'être entendu aux procédures susceptibles de conduire à une décision de retour³⁸. Dans le contexte

³⁵ Contrôleur européen de la protection des données, *Opinion 9/2025*, préc., p. 6-7 et 10.

³⁶ CEPD, *Guidelines 01/2022 on Data Subject Rights – Right of Access*, version 2.1, adoptées le 28 mars 2023, p. 9-11.

³⁷ CJUE, grande chambre, 21 juin 2022, *Ligue des droits humains ASBL c. Conseil des ministres*, C-817/19, EU:C:2022:491, points 112-118, 125-130, 167-178 et 210-214.

³⁸ CJUE, 11 décembre 2014, *Khaled Boudjlida c. Préfet des Pyrénées-Atlantiques*, C-249/13, EU:C:2014:2431.

d'une coopération biométrique UE-Maroc, cela signifie que la personne concernée doit pouvoir accéder, au moins dans une mesure suffisante, aux motifs de la décision, contester l'exactitude des données utilisées, demander la rectification ou l'effacement d'une donnée erronée, et obtenir un contrôle juridictionnel effectif sur la base légale du traitement, sa finalité, sa nécessité et sa proportionnalité. La doctrine relative à l'essence des droits fondamentaux rappelle, à cet égard, que le droit au recours effectif ne peut pas être vidé de son contenu par une organisation procédurale qui rendrait la contestation impossible ou illusoire (Lenaerts, 2019: 782-787).

L'effectivité du recours suppose toutefois une condition préalable: la personne concernée doit pouvoir connaître, au moins de manière suffisante, l'existence d'un traitement ou d'une transmission ayant contribué à une décision défavorable. Cette connaissance peut résulter d'une information individuelle lorsque celle-ci est possible, de la motivation d'une décision de refus d'entrée, de retour ou de réadmission, de l'exercice du droit d'accès auprès de l'autorité responsable du traitement, ou encore de l'intervention d'une autorité indépendante lorsque certaines informations ne peuvent pas être directement communiquées pour des raisons légalement justifiées. À défaut d'un tel point d'entrée informationnel, le recours devient largement théorique: la personne ne peut contester ni la base juridique de la transmission, ni l'exactitude des données utilisées, ni la proportionnalité du traitement, ni l'autorité effectivement responsable de l'opération informationnelle.

En matière biométrique, cette exigence prend une dimension particulière: la personne doit pouvoir contester non seulement la décision finale, mais aussi la fiabilité et l'usage des données qui ont contribué à cette décision.

Une protection renforcée doit également être accordée aux personnes vulnérables. Les mineurs, les demandeurs de protection internationale, les personnes en situation de retour, les victimes de traite, les personnes malades ou traumatisées ne se trouvent pas dans une relation ordinaire avec l'administration. Ils peuvent ne pas comprendre la portée de la collecte biométrique, ne pas être en mesure d'exercer leurs droits, ou subir des conséquences particulièrement graves en cas de transfert de données vers un pays tiers. L'EDPS a expressément recommandé, dans son avis de 2025, de préciser les conditions dans lesquelles les données personnelles des enfants peuvent être transférées vers le pays de retour, en exigeant une évaluation approfondie de l'intérêt supérieur du mineur et l'absence de risque pour son bien-être³⁹. Cette exigence est pleinement transposable à la coopération UE-Maroc: les données d'un mineur ou d'une personne vulnérable ne doivent pas être traitées

³⁹ Contrôleur européen de la protection des données, *Opinion 9/2025*, préc., p. 8-9 et 11.

comme une simple donnée d'identification; elles doivent être entourées de garanties matérielles, procédurales et institutionnelles renforcées.

Les lignes directrices récentes de la FRA sur l'EES confirment l'importance d'une approche concrète des garanties. Elles insistent sur la nécessité d'informer les personnes, d'encadrer la collecte biométrique et de tenir compte des besoins spécifiques lors du déploiement du système aux frontières⁴⁰. Cette orientation est essentielle pour éviter une lecture purement formaliste de la protection des droits fondamentaux. Les garanties ne doivent pas seulement exister dans les textes; elles doivent fonctionner dans les conditions réelles du contrôle frontalier: langue compréhensible, information disponible, assistance en cas de difficulté, traitement adapté aux mineurs, prise en compte du handicap, possibilité de corriger une erreur et accès effectif aux voies de recours. La légalité biométrique se mesure donc à l'effectivité pratique des garanties.

La doctrine récente sur les technologies frontalières rappelle également que les atteintes aux droits ne se limitent pas à la vie privée et à la protection des données. Les systèmes d'intelligence artificielle, de reconnaissance faciale ou d'évaluation du risque peuvent produire des effets sur la dignité, l'autonomie, la non-discrimination, la liberté de pensée et la capacité réelle de contester une décision. Rinaldi souligne que, dans le contexte frontalier et migratoire, la vulnérabilité des personnes concernées accroît le risque d'atteinte aux droits fondamentaux, notamment lorsque les systèmes sont opaques ou difficilement contestables (Rinaldi *et al.*, 2025: 1-6, 20-25). Cette observation renforce l'idée que la coopération biométrique ne peut pas être évaluée uniquement comme une question de sécurité informatique. Elle doit être appréciée comme une forme de pouvoir administratif transnational portant sur des personnes souvent placées en situation de dépendance institutionnelle.

Appliquées au cas UE-Maroc, ces garanties permettent de formuler une grille de validité. Si la coopération se limite à une assistance technique générale, l'enjeu principal porte sur la finalité, la supervision et la prévention d'un alignement opérationnel non contrôlé. Si elle implique une communication ponctuelle de données d'identité, il faut vérifier la base légale, la minimisation et la traçabilité. Si elle comporte un transfert de données biométriques, le régime des transferts vers les pays tiers doit être pleinement respecté. Si elle repose sur un accès médié à un résultat d'identification, la nature du résultat transmis doit être qualifiée et les droits de la personne doivent rester effectifs. Si elle produit une

⁴⁰ Agence des droits fondamentaux de l'Union européenne, *Entry/Exit System: Fundamental Rights Guidance for Border Guards*, 8 octobre 2025; Agence des droits fondamentaux de l'Union européenne, *Entry/Exit System: Fundamental Rights Guidance for Managers*, 8 octobre 2025.

externalisation fonctionnelle du contrôle, il faut examiner la chaîne de responsabilité dans son ensemble, car l'absence d'accès direct aux bases européennes ne suffit pas à exclure toute atteinte aux droits fondamentaux.

La validité juridique de la coopération biométrique dépend donc moins de son intitulé que de ses effets. Une coopération présentée comme technique peut avoir des conséquences décisives. Une donnée présentée comme limitée peut fonder une mesure de retour. Une information transmise à une autorité consulaire peut contribuer à établir une nationalité ou à délivrer un document de voyage. Une correspondance biométrique peut orienter une décision administrative. C'est pourquoi les garanties fondamentales doivent accompagner chaque étape: collecte, enregistrement, consultation, communication, transfert, conservation, usage décisionnel et recours.

Il faut enfin souligner que ces garanties ne bloquent pas par principe toute coopération biométrique. Elles en déterminent les conditions de légitimité. Une coopération fondée sur une base légale claire, des finalités strictes, une minimisation réelle, une conservation limitée, une traçabilité complète, une supervision indépendante et des recours effectifs peut être juridiquement envisageable. En revanche, une coopération fondée sur des arrangements opaques, des finalités extensibles, des échanges non documentés, des durées de conservation incertaines ou des droits difficilement exerçables ne saurait satisfaire aux exigences de la Charte. Le contrôle de validité doit donc être concret, mécanisme par mécanisme (Moreno-Lax, 2020: 385-416).

Ainsi, les garanties fondamentales ne sont pas un correctif extérieur à la coopération biométrique; elles en constituent la condition de validité juridique. Dans la coopération UE-Maroc, elles permettent de distinguer ce qui relève d'une coopération migratoire admissible de ce qui pourrait devenir une externalisation informationnelle insuffisamment contrôlée. Elles imposent de maintenir une exigence de légalité, de finalité, de nécessité, de proportionnalité, de supervision et de recours, précisément parce que la biométrie transforme l'identité corporelle en ressource administrative. C'est à cette condition seulement que la projection externe de la gouvernance migratoire européenne peut être conciliée avec la protection effective de la vie privée, des données personnelles et du droit au recours.

IV. CONCLUSION

L'analyse de la projection externe des frontières intelligentes de l'Union européenne à travers la coopération UE-Maroc montre que la question juridique ne peut être réduite à l'existence ou non d'un transfert direct de données biométriques. L'absence d'accès marocain aux systèmes européens

d'information ne suffit pas à épuiser le problème. Entre le transfert formel et l'absence totale de circulation informationnelle, plusieurs formes intermédiaires peuvent produire des effets juridiques: accès médié, communication ponctuelle, transmission d'un résultat d'identification, assistance technique ou externalisation fonctionnelle du contrôle.

Cette typologie permet de déplacer l'analyse. Il ne s'agit pas d'affirmer l'existence d'un flux généralisé de données biométriques entre l'Union et le Maroc, mais d'identifier les mécanismes par lesquels la rationalité informationnelle des frontières intelligentes peut être projetée au-delà de l'espace institutionnel de l'Union. La coopération migratoire extérieure devient alors juridiquement sensible non seulement lorsqu'elle organise un transfert de données, mais aussi lorsqu'elle produit des effets d'identification, d'orientation, de retour ou de réadmission à partir d'informations issues ou inspirées de l'architecture européenne du contrôle.

Dans cette perspective, les garanties fondamentales ne constituent pas un élément extérieur à la coopération migratoire; elles en conditionnent la validité. La légalité, la limitation des finalités, la nécessité, la proportionnalité, la supervision indépendante, la traçabilité des traitements et le recours effectif doivent être appréciés mécanisme par mécanisme. Plus la coopération produit des effets individualisés sur les personnes concernées, plus l'exigence de contrôle juridique doit être élevée.

Le cas UE-Maroc révèle ainsi l'enjeu central des frontières intelligentes: leur puissance ne réside pas seulement dans les bases de données elles-mêmes, mais dans leur capacité à structurer des pratiques de contrôle, d'identification et de coopération au-delà du territoire européen. La frontière intelligente n'est donc juridiquement admissible que si ses effets informationnels demeurent identifiables, limités, traçables et effectivement contestables.

À ce titre, la validité de chaque mécanisme peut être appréciée à partir d'une grille cumulative: existence d'une base juridique suffisamment claire; détermination précise de la finalité poursuivie; nécessité concrète du recours à la donnée biométrique ou au résultat d'identification; proportionnalité de l'information communiquée; limitation de la durée de conservation; traçabilité des accès et des transmissions; identification du responsable du traitement; contrôle par une autorité indépendante; et possibilité effective pour la personne concernée d'exercer ses droits d'accès, de rectification, d'effacement et de recours. Cette grille doit être appliquée différemment selon qu'il s'agit d'une assistance technique générale, d'une communication ponctuelle de données, d'un accès médié à un résultat d'identification, d'un transfert direct ou d'une externalisation fonctionnelle du contrôle.

L'analyse révèle cependant plusieurs lacunes normatives. La première tient à la fragmentation des instruments applicables: la coopération migra-

toire extérieure repose souvent sur une combinaison de droit dérivé, de droit souple, de financements européens, d'arrangements opérationnels et de pratiques administratives, sans toujours offrir une base juridique immédiatement lisible pour les personnes concernées. La deuxième lacune concerne l'identification du responsable du traitement lorsque plusieurs acteurs interviennent dans une même chaîne d'identification, notamment autorités européennes, autorités nationales, agences de l'Union et autorités d'un État tiers. La troisième réside dans l'effectivité du recours: si la personne ignore qu'une information, une correspondance ou un résultat d'identification a contribué à une décision défavorable, le droit au recours risque de demeurer abstrait.

Ces limites ouvrent enfin une feuille de route pour les recherches futures. Il conviendrait d'abord d'étudier empiriquement les pratiques concrètes d'identification dans les procédures de retour, de réadmission et de délivrance des laissez-passer consulaires. Il serait ensuite utile de comparer le cas UE-Maroc avec d'autres partenariats migratoires conclus par l'Union avec des États tiers situés sur les routes migratoires africaines et méditerranéennes. Il faudrait enfin approfondir le rôle des agences européennes, notamment Frontex, eu-LISA et Europol, dans la production d'effets informationnels extérieurs, même lorsque le transfert formel de données biométriques n'est pas établi.

Bibliographie

- Aden, Hartmut (2020). Interoperability between EU Policing and Migration Databases: Risks for Privacy. *European Public Law*, 26 (1), 93-108. Disponible sur: <https://doi.org/10.54648/EURO2020006>.
- Amoore, Louise (2020). *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham: Duke University Press.
- Argyriou, Vasilis et Leese, Matthias (2026). «Migrant Data Can Never Be Accurate»: Studying migration and borders through the notion of data quality. *Journal of Ethnic and Migration Studies*, 52 (7), 1615-1633. Disponible sur: <https://doi.org/10.1080/1369183X.2025.2600050>.
- Billet, Claire (2020). Les agences de l'UE et les données numériques relatives aux migrants et réfugiés. Dans Serge Turgis (dir.). *Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (p. 65-79). Rennes: Presses Universitaires de Rennes.
- Blasi Casagran, Cristina (2021). Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU. *Human Rights Law Review*, 21 (2), 433-457. Disponible sur: <https://doi.org/10.1093/hrlr/ngaa057>.
- Boizard, Maryline (2020). Les durées de conservation des données des migrants et des réfugiés. Dans Serge Turgis (dir.), *Les données numériques des migrants et des*

- réfugiés sous l'angle du droit européen* (pp. 117-126). Rennes: Presses Universitaires de Rennes.
- Brouwer, Evelien (2020). Large-scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection. *European Public Law*, 26 (1), 71-92. Disponible sur: <https://doi.org/10.54648/EURO2020005>.
- Carrera, Sergio (2016). *Implementation of EU Readmission Agreements: Identity Determination Dilemmas and the Blurring of Rights*. Cham: Springer.
- Carrera, Sergio; Cassarino, Jean-Pierre; El Qadim, Nora; Lahlou, Mehdi et Den Hertog, Leonhard (2016). EU-Morocco Cooperation on Readmission, Borders and Protection: A Model to Follow? *CEPS Paper in Liberty and Security in Europe*, 87.
- De Terwangne, Cécile (2020). Les droits fondamentaux à la vie privée et à la protection des données personnelles des migrants et des réfugiés. Dans Serge Turgis (dir.). *Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (pp. 97-116). Rennes: Presses Universitaires de Rennes.
- El Qadim, Nora (2018). Lutte contre l'immigration irrégulière et conditionnalité de l'aide au développement. *Migrations Société*, 171, 109-125.
- Faustini Torres, Luisa (2026). Bolstering Autocracy, Hindering Democracy: Local Stakeholders' Perspectives on the Effects of EU Migration Policy Externalization in Morocco. *International Migration Review*, 60 (2), 677-703. Disponible sur: <https://doi.org/10.1177/01979183251314854>.
- Fleury Graff, Thibaut (2020). La «preuve numérique» dans le contentieux de l'asile. Dans Serge Turgis (dir.). *Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (pp. 175-187). Rennes: Presses Universitaires de Rennes.
- Frasca, Eleonora (2022). L'instrumentalisation de la politique européenne des visas comme levier de la coopération en matière de réadmission: qui est sanctionné par ce mécanisme de conditionnalité négative? *Annuaire de Droit de l'Union Européenne*, 163-173.
- Frowd, Philippe M. (2018). *Security at the Borders: Transnational Practices and Technologies in West Africa*. Cambridge: Cambridge University Press.
- Gazzotti, Lorena; Jiménez Álvarez, María Gabriela et Espiñeira, Keina (2023). A «European» Externalisation Strategy? A Transnational Perspective on Aid, Border Regimes, and the EU Trust Fund for Africa in Morocco. Dans Claudia Finotelli et Irene Ponzio (dir.). *Migration Control Logics and Strategies in Europe* (pp. 69-89). Cham: Springer.
- Hijmans, Hielke (2016). *The European Union as Guardian of Internet Privacy: The Story of Art. 16 TFEU*. Vienna: Springer.
- Jeandesboz, Julien (2016). Smartening Border Security in the European Union: An Associational Inquiry. *Security Dialogue*, 47 (4), 292-309. Disponible sur: <https://doi.org/10.1177/0967010616650226>.
- Kontak, Matija (2024). Biometric Borders Envisaged by Frontex: Fundamental Rights in the BACKSEAT. *European Papers – A Journal on Law and Integration*, 9 (2), 621-640. Disponible sur: <https://doi.org/10.15166/2499-8249/773>.

- Kuner, Christopher (2013). *Transborder Data Flow Regulation and Data Privacy Law*. Oxford: Oxford University Press.
- La Spina, Encarnación (2026). The «smart» metamorphosis of borders and their ambivalent scope in the European migration control: A line in the sand. *Oñati Socio-Legal Series*, 16 (3), 1040-1070. Disponible sur: <https://doi.org/10.35295/osls.iisl.2418>
- Leese, Matthias; Noori, Simon et Scheel, Stephan (2022). Data Matters: The Politics and Practices of Digital Border and Migration Management. *Geopolitics*, 27 (1), 5-25. Disponible sur: <https://doi.org/10.1080/14650045.2021.1940538>.
- Lenaerts, Koen (2019). Limits on Limitations: The Essence of Fundamental Rights in the EU. *German Law Journal*, 20 (6), 779-793. Disponible sur: <https://doi.org/10.1017/glj.2019.62>.
- Lynskey, Orla (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.
- Marin, Luisa (2020). The Cooperation Between Frontex and Third Countries in Information Sharing: Practices, Law and Challenges in Externalizing Border Control Functions. *European Public Law*, 26 (1), 157-180. Disponible sur: <https://doi.org/10.54648/EURO2020009>.
- Michéa, Frédérique (2020). Les finalités des systèmes d'information européens à vocation migratoire. L'Union européenne et la tentation du panoptique. Dans Serge Turgis (dir.). *Les données numériques des migrants et des réfugiés sous l'angle du droit européen* (pp. 37-63). Rennes: Presses Universitaires de Rennes.
- Moreno-Lax, Violeta (2020). The Architecture of Functional Jurisdiction: Unpacking Contactless Control — On Public Powers, *S.S. and Others v. Italy*, and the «Operational Model». *German Law Journal*, 21 (3), 385-416. Disponible sur: <https://doi.org/10.1017/glj.2020.25>.
- Mutlu, Can E.; Frowd, Philippe M. et Muller, Benjamin J. (2025). The Appification of Borders: Data, Migration and Digitalization. *Big Data and Society*, 12 (2), 1-13. Disponible sur: <https://doi.org/10.1177/20539517251319996>.
- Nicolosi, Salvatore Fabio (2024). Externalisation of Migration Controls: A Taxonomy of Practices and Their Implications in International and European Law. *Netherlands International Law Review*, 71 (1), 1-20. Disponible sur: <https://doi.org/10.1007/s40802-024-00253-9>.
- Pelizza, Annalisa; Loschi, Chiara; Olivieri, Lorenzo; Trauttmansdorff, Paul et Van Rossem, Wouter Rudi (2024). Manifesto on the Datafication of Mobility Across Borders. *Engaging Science, Technology, and Society*, 10 (3), 207-215. Disponible sur: <https://doi.org/10.17351/ests2023.2831>.
- Rinaldi, Alberto et Teo, Sue Anne (2025). The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights. *International and Comparative Law Quarterly*, 74 (1), 61-89. Disponible sur: <https://doi.org/10.1017/S0020589325000090>.
- Rousvoal, Laurent (2020). L'accès des services répressifs aux données de migrants et réfugiés présentes dans le fichier Eurodac. Dans Serge Turgis (dir.). *Les données*

- numériques des migrants et des réfugiés sous l'angle du droit européen* (pp. 81-94). Rennes: Presses Universitaires de Rennes.
- Sibley, Anna et Chappart, Pascaline (2024a). Esquisse de l'automatisation du contrôle des frontières. *Plein Droit*, 140, 11-14. Disponible sur: <https://doi.org/10.3917/pld.140.0013>.
- Sibley, Anna et Chappart, Pascaline (2024b). Frénésie sécuritaire: l'algorithme du rejet. *Plein Droit*, 140, 3-6. Disponible sur: <https://doi.org/10.3917/pld.140.0005>.
- Strik, Tineke (2023). EU External Cooperation on Migration: In Search of the Treaty Principles. *European Papers – A Journal on Law and Integration*, 8 (2), 905-929. Disponible sur: <https://doi.org/10.15166/2499-8249/694>.
- Tassinari, Francesca (2021). The Externalization of Europe's Data Protection Law in Morocco: An Imperative Means for the Management of Migration Flows. *Peace and Security – Paix et Sécurité Internationales*, 9. Disponible sur: https://doi.org/10.25267/Paix_secur_int.2021.i9.1504.
- Vavoula, Niovi (2020). Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals? *European Public Law*, 26 (1), 131-156. Disponible sur: <https://doi.org/10.54648/EURO2020008>.
- Vavoula, Niovi (2024). Algorithmic accountability through the «human over the loop» in interoperable and EU AI-reliant large-scale IT systems for migration and security. *European Papers – A Journal on Law and Integration*, 9 (3), 1228-1249. Disponible sur: <https://doi.org/10.15166/2499-8249/807>.
- Wojnowska-Radzińska, Julia (2019). Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) versus data protection: Is it done in the right way? *Review of European and Comparative Law*, 37 (2), 121-138. Disponible sur: <https://doi.org/10.31743/recl.4829>.