COMPENDIUM DES NATIONS UNIES SUR LES PRATIQUES RECOMMANDEES

NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME
Centre de l'ONU pour la lutte contre le terrorisme

DIRECTION EXÉCUTIVE
DU COMITÉ CONTRE LE TERRORISME (DECT)
DU CONSEIL DE SÉCURITÉ DES NATIONS UNIES

BIOMETRICS INSTITUTE

COMPENDIUM DES NATIONS UNIES SUR LES PRATIQUES RECOMMANDEES

Compilé par DECT et UNOCT en 2018

COMPENDIUM DES NATIONS UNIES SUR LES PRATIQUES RECOMMANDEES

Pour l'usage et le partage responsables de la Biométrie pour la lutte contre le terrorisme

en association avec le Biometrics Institute

Table des matières

Synthèse

Ce compendium offre un aperçu général de haut niveau de la technologie biométrique et des systèmes d'exploitation dans le contexte de la lutte contre le terrorisme. Il est principalement destiné aux États membres n'ayant pas ou peu d'expérience des applications biométriques et également susceptibles de rencontrer des défis en termes d'assistance technique et de constitution de capacités lors de la mise en œuvre de cette technologie.

Pour un complément de lecture, des références complètes sont prévues à la fin de chaque section, accompagnées d'une synthèse des pratiques recommandées. Des études de cas sont exposées au fil du compendium afin d'offrir des exemples de bonnes pratiques et des technologies émergentes.

La première section présente les principaux éléments de la technologie biométrique et de la gestion de l'identité, notamment l'usage étendu de la biométrie dans les domaines de la criminalistique et des enquêtes des forces de l'ordre ainsi que le surcroît de complexité inhérent.

La section suivante traite de la gouvernance et des exigences réglementaires relatives à la technologie biométrique selon les perspectives du droit international, des droits de l'homme, des examens éthiques, des exigences de protection des données et du droit à la vie privée. Elle est suivie par un examen global des vulnérabilités potentielles des systèmes biométriques et de certaines mesures de contrôle servant à atténuer les risques. Les normes opératoires techniques et scientifiques internationales sont ensuite appréciées. Elles couvrent la certification et l'accréditation des applications biométriques mais aussi les systèmes de management de la qualité employés pour les processus criminalistiques associés. La dernière partie de cette section traite des achats, de la maintenance et des exigences de ressources d'un réseau ou d'un système biométrique de lutte contre le terrorisme et, en particulier, des décisions clés opérationnelles et financières qui s'imposent à l'heure de l'évaluation d'un potentiel système nouveau ou étendu.

La section finale propose un aperçu général des bases de données et systèmes biométriques de lutte contre le terrorisme actuels, à l'échelle du spectre des applications de maintien de l'ordre, de gestion des frontières et militaires. Elle considère aussi les avantages du partage des données biométriques à un échelon bilatéral, multilatéral, régional et global et sur la manière dont les données biométriques, si elles sont employées avec d'autres données de renseignement, peuvent être exploitées de manière proactive afin d'empêcher des actes de terrorisme outre leur rôle traditionnel d'outil d'enquête. Les mesures prises par les autorités, en résultante de correspondances biométriques, sont alors appréciées à l'aune du droit international des droits de l'homme et de la nécessité d'une intervention légale et proportionnée en toute connaissance de cause. La partie finale de la section traite de l'inclusion de la biométrie dans les stratégies de lutte contre le terrorisme des États membres et des Régions et du rôle essentiel des organismes des forces de l'ordre et de contrôle des frontières dans le soutien actif de ces stratégies.

Le compendium est un document vivant et ses versions sont contrôlées aux fins suivantes :

- préserver son caractère actuel et réactif face au rythme effréné de l'innovation technologique et du développement scientifique dans le domaine de la biométrie et
- être évolutif et pertinent face aux menaces émergentes et en évolution permanente du terrorisme international.

Préface

La résolution 2322 (2016) du Conseil de sécurité relative au renforcement de la coopération internationale des forces de l'ordre et des autorités judiciaires en matière de lutte contre le terrorisme appelle explicitement les États membres à partager les informations — notamment les informations biométriques et biographiques — sur les combattants terroristes étrangers (CTE) et autres individus ou organisations terroristes. Dans sa résolution 2396 (2017), le Conseil a décidé que les États Membres devaient élaborer et mettre en œuvre des systèmes de collecte de données biométriques, notamment d'empreintes digitales, de photographies, de reconnaissance faciale et d'autres données biométriques d'identification pertinentes, pour identifier avec certitude et de manière responsable les terroristes, y compris les CTE, dans le respect du droit international des droits de l'homme et du droit national. Le Conseil encourage également les États à partager ces données de manière responsable avec d'autres États ainsi qu'avec l'Organisation internationale de police criminelle (INTERPOL) et les autres organismes internationaux compétents.

L'échange efficace des données biométriques est vital pour les enquêtes sur la criminalité transnationale et pour l'identification des terroristes. Dans le cadre des enquêtes liées au terrorisme, les techniques biométriques et autrement criminalistiques peuvent grandement aider les enquêteurs et le ministère public, notamment en établissant des liens entre un individu et une activité, un événement, un lieu, une substance ou un autre individu spécifique. Le renforcement de la capacité des États Membres dans ce domaine s'avère dès lors crucial.

Ce compendium de bonnes pratiques et de recommandations a été développé par le Groupe de travail sur la gestion des frontières et les forces de l'ordre en matière de lutte contre le terrorisme de la CTITF (Counter-Terrorism Implementation Task Force - Équipe spéciale de lutte contre le terrorisme) avec le soutien financier du Centre des Nations Unies pour la lutte contre le terrorisme (UNCCT - UN Counter-Terrorism Centre), sous l'égide du Bureau de lutte contre le terrorisme (BLT) des Nations Unies. Le compendium traite de questions cruciales comme la gouvernance, la réglementation, la protection des données, la politique relative à la vie privée, les droits de l'homme mais aussi la gestion du risque et les appréciations de la vulnérabilité.

Les Gouvernements doivent traiter les implications de cette technologie pour les droits de l'homme afin de protéger les individus identifiés dans ces systèmes contre tout abus et de s'assurer que les actions entreprises lors de la planification, puis ultérieurement, sont menées à bien dans le respect des obligations inhérentes au droit international tel qu'il est consacré dans les instruments internationaux et régionaux relatifs aux droits de l'homme. Comme toutes les mesures de sécurité, la biométrie présente des vulnérabilités. La manière dont les vulnérabilités des systèmes sont identifiées, comprises et minimisées s'avère dès lors cruciale. Une conception minutieuse, un enregistrement exact des données biométriques et une méthodologie de définition des paramètres de correspondance s'avèrent donc primordiaux pour son succès. Une diversité de technologies, aussi bien logicielles que matérielles, peuvent servir à détecter, à contrecarrer et à réduire le risque d'attaques par usurpation[1].

Le Compendium a été développé en partenariat avec le Biometrics Institute, une organisation à but non lucratif de promotion d'un usage responsable et éthique de la biométrie, servant de forum indépendant et impartial pour les utilisateurs de la biométrie et les autres parties intéressées. Le

[1] Une attaque par 'Usurpation' (aussi dénommée attaque de présentation) correspond à la présentation de fausses données biométriques (ainsi un masque facial en latex, une photographie, une fausse empreinte digitale ou vocale) d'un utilisateur inscrit légitime pour obtenir un accès sans autorisation à un système de reconnaissance biométrique.

Biometrics Institute coopère étroitement avec la Direction exécutive du Comité contre le terrorisme (DECT) afin de former un consortium international d'experts afin de guider l'élaboration du compendium, notamment des experts gouvernementaux et des experts en biométrie forts d'une expérience en lutte contre le terrorisme, maintien de l'ordre, gestion des frontières, technologie biométrique et protection des données et de la vie privée.

Le Compendium a été élaboré dans le cadre d'un projet à long terme destiné au renforcement de la capacité des États et des entités internationales et régionales concernées par la collecte, l'enregistrement et le partage des informations biométriques sur les terroristes, notamment les CTE, conformément aux résolutions du Conseil de sécurité susmentionnées. Ce projet Biométrie est mis en œuvre par la DECT en coopération avec les entités du CTITF ainsi INTERPOL, l'Office des Nations Unies contre la drogue et le crime (ONUDC), l'Organisation de l'aviation civile internationale (OACI) et le Haut-Commissariat des Nations Unies pour les réfugiés (UNHCR). Les objectifs du projet porte sur la sensibilisation des initiatives régionales et internationales afin de promouvoir l'usage de la biométrie, le renforcement de la coopération et de la coordination entre les entités concernées, la croissance de l'usage et du partage de la biométrie à l'échelon global, notamment par la promotion de l'inclusion systématique des informations biométriques liées aux profils terroristes dans les notices et bases de données d'INTERPOL et dans la progression de l'efficacité de l'assistance procurée aux États membres dans ce domaine,

Vladimir Voronkov
Secrétaire général adjoint
Bureau de lutte contre le terrorisme des Nations Unies
Directeur exécutif
Centre de lutte contre le terrorisme des Nations Unies

Michèle Coninsx
Sous-Secrétaire générale
Directrice exécutive
Direction exécutive du Comité contre le terrorisme

À propos du Biometrics Institute

Organisation à but non lucratif promouvant l'usage responsable et éthique de la biométrie, le Biometrics Institute saisit l'opportunité de soutenir ce projet. Le Biometrics Institute offre un forum international indépendant et impartial pour les utilisateurs de la biométrie et autres parties intéressées. So rôle est d'instruire et d'informer ses membres, ses parties prenantes clés et le public sur la biométrie, de soutenir le développement et la sensibilisation sur les normes, politiques et bonnes pratiques et de promouvoir la sécurité et l'intégrité des programmes et systèmes biométriques.

Il a été créé en 2001 et compte des bureaux à Londres et Sydney. Ses adhérents, comptant plus de 230 organisations de 30 pays différents, couvrent un vaste éventail d'utilisateurs comme les organismes publics, les autorités de maintien de l'ordre et de gestion des frontières, les banques et compagnies aériennes mais aussi les chercheurs, fournisseurs et experts en confidentialité. L'Institut ne promeut pas la technologie biométrique mais porte l'accent sur l'usage responsable des systèmes biométriques, sur leur sécurité et leur intégrité et, plus crucialement, sur la protection des données et de la vie privée. L'Institut reconnaît que les systèmes biométriques présentent des vulnérabilités inhérentes qui doivent être identifiées et atténuées.

Biométrie et droits de l'homme et de la vie privée

La biométrie devient omniprésente alors que, simultanément, le public a développé une acceptation supérieure de la technologie à travers l'usage de la biométrie sur les téléphones portables mais sans nécessairement être conscient des implications. La nécessité d'un surcroît de formation sur les avantages et les risques des applications biométriques devient dès lors manifeste. La biométrie sait se montrer pratique et peut offrir un niveau élevé de sécurité. Cependant, des défis demeurent ainsi la protection du droit à la vie privée, la protection des données et la lutte contre les attaques par usurpation. Les données à caractère personnel, comme les données biométriques, devraient uniquement être recueillies et enregistrées si cela s'avère nécessaire et proportionné.

La biométrie doit assumer un rôle d'une importance croissante dans la lutte contre le terrorisme à l'échelle de la planète, ainsi afin de lutter contre la fraude, le vol d'identité et autres délits employés par les terroristes au service de leurs opérations. Toutefois, afin de prendre conscience du plein potentiel de la biométrie, les gouvernements doivent aussi assurer que les individus identifiés par de tels systèmes sont protégés et que la collecte, le stockage et l'usage des données biométriques se déroulent dans le respect du droit international des droits de l'homme et de la législation relative à la vie privée, notamment le Pacte international relatif aux droits civils et politiques (PIDCP) et à la Déclaration universelle des droits de l'homme (DUDH) des NU.

Les personnes dont la biométrie ou l'identité a été volée ou simplement victimes d'une erreur du système doivent être protégées. Le rétablissement de l'identité d'une personne n'est pas aussi simple que la réinitialisation d'un mot de passe. Votre biométrie ne vous quitte pas de toute votre vie et une prudence absolue s'impose. Ce compendium énonce les questions et solutions possibles pour cette tâche difficile de l'alliance de stratégies efficaces de lutte contre le terrorisme et des droits de l'homme, notamment du droit à la vie privée.

Vulnérabilités et attaques des systèmes biométriques

Comme toutes les mesures de sécurité, la biométrie présente des vulnérabilités. La manière dont les vulnérabilités des systèmes sont minimisées s'avère cruciale. Une conception minutieuse, un enregistrement exact des données biométriques et une méthodologie de définition des paramètres

de correspondance s'avèrent donc primordiaux pour son succès. Des paramètres trop exigeants peuvent générer de 'faux négatifs', refusant l'accès à un utilisateur authentique. S'ils sont insuffisants, de 'faux positifs' peuvent autoriser l'accès des utilisateurs frauduleux.

Le Biometrics Institute emploie des précautions raisonnables pour assurer l'exactitude des éléments présentés dans ce compendium. Du fait du contenu et des saisies variables durant et après le processus de mise en œuvre de la technologie biométrique, l'Institut ne peut être tenu responsable des résultats ou de la conformité. Le compendium a été préparé uniquement à des fins d'information et n'est pas censé constituer un avis juridique ou de conformité.

Andrew Rice
Président et Directeur
Biometrics Institute

Isabelle Moeller
Directrice exécutive
Biometrics Institute

1. Introduction aux systèmes biométriques et à l'identité

La section 1 présente les principaux éléments de la technologie biométrique et de la gestion de l'identité, notamment l'usage étendu de la biométrie dans les domaines de la criminalistique et des enquêtes des forces de l'ordre ainsi que le surcroît de complexité qui en découle.

Les humains sont des animaux sociaux dotés d'une aptitude exceptionnelle à reconnaître - et donc distinguer - les personnes familières. Simultanément, les humains ont un fort sentiment du soi et de leur caractère unique en tant qu'individus. Nos instincts sociaux servent à nous percevoir en tant qu'individus uniques et à reconnaître l'individualité d'autrui. Au niveau biologique, les humains sont (à des fins pratiques) uniques. Cependant, notre « moteur de reconnaissance humaine » ne fonctionne pas biologiquement. En fait, les humains fonctionnent mal à l'heure de distinguer les personnes qui ne leur sont pas familières. Les systèmes d'identité employés par les humains ne fonctionnent pas non plus à l'aide de la biologie. En lieu et place, ils exploitent des combinaisons d'attributs identitaires et d'attributs contextuels en tant que marqueurs représentatifs mais distincts de l'entité biologique décrite[2].

Les attributs identitaires incluent les noms, date et lieu de naissance, nationalité, genre et identificateurs[3] biométriques. Les attributs contextuels sont des informations transactionnelles, communément connexes à un moment et un lieu. L'usage des attributs contextuels rehausse l'assurance de l'identité. Les attributs identitaires peuvent être biographiques ou biométriques et, dans certaines circonstances, être sujets au changement. Ainsi, la mutabilité des attributs identitaires biographiques peut inclure :

- Noms – sujets à la translittération, soit un même nom peut être épelé de différentes manières
- Date de naissance – sujette à un délai ou des incohérences d'enregistrement dans les registres officiels
- Lieu de naissance – représentable de maintes manières
- Genre – sujet à la préférence de l'individu, aux changements de sexe, etc.
- Citoyenneté – possiblement multiple et sujette à changements

À l'échelle du cycle de vie d'un humain, les attributs identitaires biométriques peuvent être sujets à changements, ainsi la taille relative ou la clarté et la définition des caractéristiques extractibles suite aux processus de croissance et de vieillissement, voire à la maladie. Les données biométriques de certains individus peuvent être endommagées ou manquantes. Ainsi, par exemple, les empreintes digitales se forment dès les stades initiaux de la gestation, sont immuables tout au long de la vie, sauf en cas de dommages, et se préservent pendant un temps considérable après le décès, spécialement dans des environnements chauds et secs entraînant une dessiccation de la peau. Bien que l'agencement des crêtes papillaires de la structure d'empreinte digitale demeure constant, le doigt lui-même change de taille au fil de la vie et la qualité des caractéristiques contenues dans une empreinte digitale peut se détériorer du fait d'abus environnementaux, de dommages ou du vieillissement. D'autres éléments de biométrie peuvent être affectés par des changements similaires. Par conséquent, les algorithmes modernes employés dans les applications biométriques sont conçus pour permettre des ajustements raisonnables en fonction de ces changements. De la sorte, le nombre

[2] *Identity verification- The importance of context and continuity of identity*, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

[3] En 1995, la « Biométrie » était définie par le Biometric Consortium du Gouvernement des États-Unis comme « ...la reconnaissance automatisée des individus sur la base de leurs caractéristiques comportementales et biologiques ».

de personnes pouvant être enregistrées et gérées sur un système, indépendamment des variantes d'âge ou d'une détérioration mineure de leurs caractéristiques biométriques, est maximisé.

Les marqueurs biométriques sont des attributs identitaires et, comme ils sont hautement représentatifs de l'humain qu'ils décrivent, offrent un fondement approprié pour les comparaisons numériques. Néanmoins, comme pour les attributs identitaires biographiques, un échantillon biométrique, une fois capturé en image ou transformé en modèle ou profil, est distinct de l'entité biologique qu'il décrit. La capture et l'enregistrement des attributs identitaires, notamment des attributs biométriques, sont des processus systématiquement incomplets et imparfaits et donc soumis potentiellement à l'erreur. La correspondance probabiliste inhérente aux comparaisons biométriques est sujette à la variance statistique. La présence d'une erreur ou d'une variance statistique dans les systèmes de reconnaissance des humains les rend potentiellement vulnérables à une diversité d'attaques (voir Section 2.3) sauf si des mesures de protection rigoureuses sont mises en œuvre et constamment actualisées dans le cadre d'un processus de Gestion du risque système.[4] L'atténuation de ces vulnérabilités inhérentes des systèmes de reconnaissance des humains est un volet clé de ce Compendium.

Les systèmes biométriques sont pensés pour la reconnaissance des individus selon leurs caractéristiques biologiques et physiologiques, comme les empreintes digitales, motifs des veines de la main, iris, visage, ADN et autres.[5] Chacune représente une modalité biométrique. Le choix de la ou des meilleures modalités biométriques dépend du contexte du cas d'usage d'application (voir Section 2.5). En général, les modalités biométriques partagent des caractéristiques[6] qui les rendent à un degré plus ou moins important :

- Universelles – elles se retrouvent chez tous les individus (sauf ceux présentant des caractéristiques biométriques endommagées ou manquantes).
- Uniques – elles devraient assurer la distinction des individus d'une population enregistrée. Cet aspect peut être variable pour certaines modalités, ainsi les jumeaux identiques qui partagent le même profil ADN mais dont les empreintes digitales diffèrent.
- Permanents – elles devraient être stables et invariables avec le temps en termes d'algorithme de correspondance, en tenant compte des variations causées par le cycle de vie humain.
- Mesurables – elles devraient pouvoir être aisément acquises et numérisées par le système.
- Efficaces – elles devraient être exactes, rapides et rigoureuses pour les processus d'activité primaires et de référence.
- Acceptables - elles devraient satisfaire les normes et attentes sociétales et pouvoir être utilisées par un pourcentage élevé de la population d'enregistrement prévue.
- Vulnérables au risque de contournement - les imposteurs peuvent potentiellement obtenir un accès sans autorisation en employant divers artefacts et substituts sauf si des contremesures rigoureuses sont employées et actualisées en continu.

[4] « Les systèmes de reconnaissance des humains sont par inhérence probabilistes et donc par inhérence faillibles. Le risque d'erreur est faible mais ne peut être éradiqué. Les créateurs et opérateurs de systèmes devraient anticiper et planifier les occurrences d'erreurs même si elles devraient s'avérer peu fréquentes. » page 1, *Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), disponible en téléchargement à :* http://www.nap.edu/openbook.php?record_id=12720&page=1

[5] **NB** Ce Compendium traite principalement de la biométrie physique, associée à l'identité humaine (visage, empreintes digitales, ADN, etc.) et non pas comportementale. La biométrie comportementale inclut des modalités comme la démarche, l'usage caractéristique du clavier et de la souris, les signatures écrites et autres qui mesurent des modèles d'activité humaine.

[6] Liste adaptée de Jain et al. « Biometrics: Personal Identification in Networked Society », Norwell, Mass.: Kluwer Academic Publisher (1999)

Comme nombre de systèmes biométriques impliquent des comparaisons avec des données de référence, un facteur clé lors du choix de la modalité de prédilection tient à la disponibilité des données historiques qui sont compilées, ou peuvent l'être, sous forme de base de données de référence exploitable et utile afin d'établir et de vérifier l'identité. Les systèmes peuvent employer une modalité unique (Fonctionnalité monomodale) comme la reconnaissance faciale ou combiner les modalités (Fonctionnalité multimodale) ainsi les empreintes digitales, l'iris et le visage. Nous constatons la croissance rapide de la palette d'applications pour les systèmes biométriques dans les secteurs privé comme public, notamment :

- Registres nationaux d'État civil facilitant l'accès aux services publics locaux ou nationaux
- Permis de conduire
- Casier judiciaire
- Détection des crimes
- Vidéosurveillance
- Sécurité aux frontières /Systèmes de délivrance de passeport
- Aide aux réfugiés
- Services financiers
- Systèmes informatiques
- Accès aux bases de données sécurisées
- Accès aux sites
- Accès aux smartphones
- Gestion de l'identité des soins de santé
- Gestion de la présence sur le lieu de travail

Les modalités employées dans ces applications peuvent identifier un individu même en cas de fausses déclarations ou de tentative d'usurpation de l'identité d'une autre personne. Il s'agit d'un attribut précieux qui peut servir efficacement au suivi et à la détection des terroristes mais aussi à la mise en échec de leurs activités à l'échelon global. La biométrie est le creuset d'une culture solide et vivante de développement et de recherche commerciaux, de nouvelles applications comme de nouvelles modalités apparaissant régulièrement sur le marché.

Le modèle opératoire standard d'un système biométrique de base, ainsi celui utilisé pour le contrôle d'accès, comporte les stades suivants :

- *Acquisition et enregistrement* – obtenir un échantillon biométrique d'un individu (sujet) en utilisant un dispositif de capture de données. Le processus d'acquisition peut employer un dispositif installé sur un site fixe et permanent ou un dispositif mobile capable de télécharger des données depuis un site distant. Les données biométriques peuvent être acquises par contact avec le dispositif de capture de données (empreintes digitales), à proximité (capture en direct des images faciales) ou à distance. Cependant, le facteur critique de succès d'un quelconque système tient à la qualité des données biométriques enregistrées. Des enregistrements de mauvaise qualité réduisent manifestement les performances du système. Il est donc crucial d'acquérir des données biométriques d'une qualité constamment élevée afin d'optimiser la capacité de correspondance (voir Section 2.3.3.).
- *Extraction de données* – conversion de l'échantillon acquis dans un modèle biométrique, ainsi une image d'empreinte digitale peut être traitée sous forme de matrice numérique de nombres à des fins de stockage, de recherche et de comparaison. Le processus d'extraction de données est donc conçu pour transformer l'image brute ou l'échantillon d'origine en

ensemble exploitable et efficient de données numériques, susceptible d'être interrogé et comparé exactement avec des modèles de référence dans la base de données tout en nécessitant un espace de stockage significativement moindre dans le système que celui occupé par l'échantillon /image biométrique d'origine.

- *Stockage de données* – rétention des données enregistrées dans le système ou la base de données, parfois limitée à un seul modèle par personne une fois la phase de recherche /comparaison terminée. Pour la plupart, les dispositifs de capture de données chargent des données vers un serveur ou une base de données centralisée pour la recherche. Cependant, certains dispositifs mobiles disposent de leur propre base de données intégrée de sorte qu'ils peuvent être déployés à distance sans besoin de connexion à un quelconque autre équipement.
- *Comparaison de données* – accès à la base de données et extraction d'un ou plusieurs modèles enregistrés préalablement pour la comparaison avec le modèle de requête présenté.
- *Correspondance de données* – usage d'algorithmes informatiques afin de déterminer si le modèle de requête correspond aux modèles de base de données sélectionnés. Les modèles de requête ne sont pas normalement conservés après leur correspondance avec un modèle de référence dans la base de données.
- *Produit* – le résultat de correspondance, ou non, contribue au fonctionnement du système dans son ensemble ainsi lorsque le composant biométrique est conçu pour vérifier une déclaration d'identité des entrées de la base de données pour la légitimité de l'accès à un bâtiment sécurisé. Une correspondance autoriserait donc l'accès sur la base de la vérification avec un modèle d'identités déclarées alors qu'un défaut de correspondance aboutirait à un refus d'accès.

Cependant, toutes les applications n'utilisent pas nécessairement des identités déclarées car les systèmes biométriques emploient deux processus fondamentalement différents. Le premier processus employant l'identité déclarée est la :

Vérification – (aussi dénommée comparaison un contre un ou 1:1). Ce modèle utilise une identité déclarée afin de sélectionner un seul modèle de la base de données ou du document électronique pour le comparer avec le modèle de requête. Ce processus compare le modèle de requête avec le modèle de la base de données et confirme, ou infirme, que les deux modèles proviennent de la même personne.
La vérification pose la question : « Êtes-vous la même personne que celle dont l'identité a déjà été authentifiée et enregistrée dans la base de données ? ».

Le second processus, un modèle de recherche, est une :

Identification – (aussi dénommée comparaison 1 à plusieurs ou 1:n). Cette fonction de recherche ne dépend pas d'une identité suggérée. Le modèle de requête interroge donc la base de données intégrale en quête d'une correspondance possible. Le logiciel de recherche et de correspondance génère un score de similarité pour des correspondances potentielles et soit sélectionne automatiquement une correspondance à la certitude élevée, soit présente une liste candidate de correspondances suggérées à un opérateur humain pour comparaison avec le modèle de requête.
L'identification pose la question : « Êtes-vous dans la base de données de référence et, si c'est le cas, à quel enregistrement correspondez-vous ? ».

La valeur et le contexte des produits des systèmes de vérification ou d'identification dépendent du modèle opératoire de l'application. Par exemple, dans certains cas, une identification positive

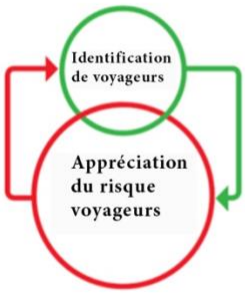
correspondrait à un produit de routine où un résultat négatif serait l'exception (ainsi l'accès du personnel à une zone sécurisée) mais, pour d'autres modèles, un produit négatif serait une attente normale alors qu'un résultat positif serait l'exception (ainsi l'ensemble des passagers comparés à une liste de surveillance biométrique de terroristes). Les systèmes biométriques efficaces intègrent des tâches distinctes de vérification et d'identification pour rehausser l'assurance de l'identité et la fiabilité des comparaisons des ensembles de données de référence.

Aux yeux de l'utilisateur, nombre d'applications biométriques semblent complètement automatisées - de l'acquisition au produit - mais une intervention humaine est souvent nécessaire à divers stades du processus pour les systèmes plus complexes afin d'assurer que le système fonctionne avec fluidité même si cela n'est pas manifeste pour l'utilisateur. Cependant, du fait de la croissance continuelle et exponentielle de la puissance informatique et des nouvelles technologies de traitement, l'exigence d'intervention humaine diminue rapidement. Toutefois, bien que la correspondance automatisée des échantillons biométriques doive devenir la norme, l'association des échantillons correspondants à d'autres attributs contextuels et identitaires devrait probablement demeurer, dans les cas complexes, le sujet d'un processus de décision humaine.

Étude de cas 1 – Biométrie aux frontières

L'autorisation de passage de frontières des voyageurs via une vérification 1:1 informe et est informée par les appréciations du risque des voyageurs en employant des comparaisons 1:n avec des listes de surveillance et des ensembles de données de renseignement (voir Figure 1). Les attributs identitaires enregistrés dans les listes de surveillance et les ensembles de données de renseignement sont habituellement incomplets. Cela tient au fait que les cibles à inclure dans les listes de surveillance sont identifiées selon un éventail de circonstances et de critères différents. Les attributs biographiques ou biométriques ne peuvent pas tous être associés à chaque liste de surveillance ou de renseignement. Les attributs contextuels sont incomplets. Tous les éléments d'attribut des listes de surveillance et des ensembles de données de renseignement sont sujets à l'erreur.

Figure 1 - adaptation d'*ICAO TRIP Guide on Border Control Management, Montréal (2018)*
(Avec la permission de l'OACI)



Comparaison	Source de données de référence	Base de comparaisons biographiques	Base de comparaisons biométriques	Associations d'attributs contextuels
Vérification 1:1	Documents de voyage	• Nom • Date de naissance • Sexe • Nationalité	• Visage • Empreintes digitales • Iris	• Heure et lieu • Nationalité • Inspection de documents de voyage
Identification 1:n	- Listes de surveillance - Renseignement	• Nom • Date de naissance • Sexe • Nationalité	• Visage • Empreintes digitales • Iris • Voix • ADN	• Heure et lieu • SLTD Interpol • Événements antérieurs • Attributs d'association (portable, connexions e-mail et autres)

Les identités vérifiées contribuent à une association fiabilisée des attributs contextuels, biographiques et biométriques et donc à des recherches plus efficaces des listes de surveillance et

des bases de données de renseignement. Crucialement, les comparaisons biométriques contribuent aux résultats de correspondance d'identité mais sans les déterminer seules.[7]

1.1 Performances du système

Les performances d'un quelconque système biométrique dépendent largement de (1) la portée et l'ampleur de son usage prévu, de (2) la sélection de la ou des modalités les plus appropriées au service de cette application et du (3) traitement fiable, constant et en temps utile bénéficiant d'une exigence faible de maintenance. Les indicateurs de performances clés des systèmes biométriques sont l'exactitude, les taux d'erreur[8], le rendement et les volumes et taux de gestion des exceptions. Généralement, l'exactitude est une mesure de la capacité du système à assurer correctement la correspondance des attributs identitaires biométriques de la même personne tout en évitant les fausses correspondances des attributs identitaires biométriques de différentes personnes. Les composants suivants servent à exprimer l'exactitude d'un système biométrique, sous forme de pourcentage ou de proportion, et sont habituellement dérivés d'essais sur le terrain ou de tests en laboratoire.

Taux d'acceptation authentique (TAA) – La mesure de la capacité du système à faire correspondre correctement les attributs identitaires biométriques de la même personne.

Taux d'acceptation fausse (TAF) – Une acceptation de fausseté survient si le système fait correspondre par erreur le modèle biométrique de requête d'une personne avec le modèle biométrique d'une autre personne de la base de données. Le TAF est le nombre d'acceptations fausses en proportion du nombre total de requêtes biométriques qui auraient dû être rejetées, soit le nombre de défauts de correspondance *générés et présentés par le système* en proportion des défauts de correspondance véridiques.

Taux de rejet authentique (TRA) – La mesure du nombre d'occasions où les attributs identitaires biométriques d'une personne ne correspondent correctement *pas* aux attributs identitaires biométriques d'autres individus dans la base de données, soit la fréquence des défauts de correspondance corrects.

Taux de rejet faux (TRF) – Un rejet faux se produit si le modèle biométrique de requête ne correspond pas au modèle de base de données correct même s'ils correspondent à la même personne. Le TRF est le nombre de rejets faux en proportion du nombre total de requêtes biométriques qui auraient dû être acceptées, soit le nombre de correspondances *générées et présentées comme des défauts de correspondance par le système* en proportion des correspondances véridiques.

[7] Voir l'ICAO TRIP Guide on Border Control Management, Montréal (2018) pour en savoir plus

[8] Le calcul des taux d'erreur exige une abstraction - l'hypothèse d'un ensemble fermé - pour autoriser l'exécution ultérieure d'une comparaison tous:tous de la base de données afin de dériver et de calculer les taux d'erreur. Dans nombre de cas, ces calculs sont exécutés dans le cadre de simulations en exploitant des ensembles de données normalisés qui peuvent être représentatifs, ou non, de données en direct du monde réel. L'abstraction du taux d'erreur peut s'avérer utile pour la conception de système et pour les prévisions de performances de vérification 1:1. Dans le monde réel, face à une population globale dépassant les 7 milliards d'individus, les substitutions de l'extérieur de l'ensemble sont possibles et même, dans le cas des listes de surveillance et des ensembles de données de renseignement, probables. Les taux d'erreur doivent être employés avec précaution et appliqués uniquement à une tâche de vérification. Les performances de correspondance des systèmes biométriques dans le monde réel peuvent différer significativement de celles prédites par des simulations de taux d'erreur.

Pour la conception du système, il est donc préférable de maximiser les TAA et TRA et de minimiser à la fois le TAF et le TRF. Par exemple, en des termes simples, un réglage d'exactitude avec un TAA de 70% entraînerait un TAF de 30% alors que pour un TAA de 97%, le TAF serait de seulement 3%. Il convient de relever qu'aucun système biométrique ne fonctionne en assurant un taux d'exactitude de 100%.

Cependant, les valeurs TAF et TRF affichent aussi une relation de proximité et l'équilibre de prédilection entre ces deux taux d'erreur dépend largement de l'usage concret du système biométrique spécifique. Ainsi, lorsque l'accès d'un employé aux installations d'une compagnie est lié à une application biométrique, alors un TRF élevé empêcherait le personnel de l'entreprise d'accéder sur une base régulière. En revanche, un TAF trop élevé aboutirait à l'accès routinier d'un personnel sans autorisation. Par conséquent, l'application nécessite une valeur Seuil ajustable, assurant l'équilibre entre le TRF et le TAF pour faciliter l'accès du personnel tout en évitant les entrées sans autorisation dans la *plupart* des occasions. Si des niveaux élevés de sécurité s'imposent, le seuil devrait être réévalué pour éviter un accès sans autorisation en réduisant autant que possible le TAF même aux dépens d'une hausse du TRF, affectant donc l'accès d'un personnel légitime. Dès lors, cette valeur seuil est souvent le fruit d'un compromis pragmatique entre les TAF et TRF optimisant l'efficacité du système pour l'application prévue et pondérant le besoin de sécurité en regard de l'aspect pratique pour les utilisateurs, la vitesse de traitement et les coûts d'ensemble du système. Le Taux d'erreur égale (TEE) [9] se réfère au réglage de seuil de certaines modalités où le TRF et le TAF sont égaux, soit la proportion d'acceptations fausses est égale à la proportion de rejets faux.

D'autres facteurs affectent l'exactitude, ainsi le Taux de défaillance d'acquisition (TDA), soit en termes généraux la proportion de toutes les transactions enregistrées qui ne peuvent aboutir du fait de défaillances lors des phases de présentation (aucune image capturée), d'extraction de caractéristiques ou de contrôle qualité. Outre une défaillance du système, il inclut aussi les cas où l'individu présente des caractéristiques biométriques endommagées, blessées ou manquantes. Le TDA est une mesure importante afin de déterminer la capacité opératoire en direct d'un système. Un TDA élevé exige une approche alternative afin de capturer la biométrie des personnes dont l'enregistrement est impossible pour une raison quelconque. Cela pourrait impliquer l'usage d'une biométrie similaire mais alternative, ainsi le pouce gauche au lieu du droit ou même l'ajout d'une seconde capacité de reconnaissance biométrique différente qui pourrait nécessiter le développement d'un système multimodal. Si ces alternatives ne sont pas envisageables, alors une solution non biométrique - dénommée Gestion d'exception - pourrait être adoptée. Par exemple, ce processus pourrait exiger des individus dont l'enregistrement biométrique est impossible de faire examiner leur identité par un opérateur humain ou d'employer d'autres méthodes, potentiellement moins sécurisées, comme un code PIN ou une signature écrite, ce qui pourrait réduire l'efficacité d'ensemble du système. Les applications biométriques multimodales sont souvent favorisées pour cette raison car elles autorisent habituellement une proportion supérieure d'enregistrements tout en réduisant le TDA.

Le Rendement détermine le nombre de personnes pouvant accéder au système durant une plage horaire, soit la capacité en fonction de la vitesse. Par exemple, un aéroport exploitant un accès avec passeport électronique biométrique devrait calculer les volumes de passagers réels et prévisionnels pour installer suffisamment de portails biométriques afin de faciliter un flux efficient de passagers en cas de pic de fréquentation. Le système biométrique pourrait ainsi fonctionner avec des taux d'erreur prédéterminés pour des raisons de sécurité tout en traitant de multiples vérifications simultanées par seconde à des fins de satisfaction des usagers et d'efficience de l'activité.

[9] aussi dénommé Taux d'erreur de croisement

1.2 Le rôle de la biométrie en criminalistique

En général, la criminalistique traite du transfert du matériel physique ou des medias électroniques et numériques entre les personnes, les objets et les lieux. Ce matériel peut être visible, ainsi une tache de sang sur un mur, invisible, ainsi une preuve à l'état de trace microscopique comme un résidu d'explosif ou de tir d'arme à feu, ou encore une image électronique, ainsi un visage capturé par une caméra de vidéosurveillance. Ce matériel ou ces données peuvent être transférés avant, durant ou après un crime. Une partie de ce matériel capture aussi des caractéristiques *biométriques*, ainsi l'impression d'une empreinte digitale déposée dans de la sueur sur un verre, une voix enregistrée durant une conversation téléphonique ou encore un profil ADN créé à partir de la salive sur le bord d'une tasse. Ces 'éléments biométriques criminalistiques'[10] sont des composants clés de la criminalistique et des éléments vitaux des enquêtes des forces de l'ordre du fait de leur capacité potentielle d'identification des individus. Ils sont aussi cruciaux pour l'exécution efficace et le succès des opérations de lutte contre le terrorisme en :

- Prouvant ou réfutant l'implication d'un individu dans un délit en procurant des preuves qui l'incriminent ou l'exonèrent elles-mêmes ou en contribuant à une autre preuve (voir Étude de cas 2).
- Procurant des processus objectifs et fiables, dans le respect de la législation, réduisant la dépendance envers les aveux dans le cadre des enquêtes criminelles, spécialement s'ils sont obtenus par l'usage de la torture ou autres mesures coercitives.
- Interprétant l'activité sur des scènes de crime et les événements associés
- Reliant une personne à une activité, un événement, un lieu ou une autre personne, durant ou après un incident.
- Reliant un événement à un autre ou de multiples événements.
- Localisant et reliant des données entre différents systèmes électroniques et numériques.

Ces capacités exigent la contribution coordonnée d'autres disciplines pertinentes en criminalistique et dans les domaines de l'expertise spécialisée technique et de laboratoire. [11] Le traitement de tous les matériels criminalistiques, sur le lieu du crime et en laboratoire, devrait être mené en conformité avec les normes internationales et les systèmes de management de la qualité associés (voir Section 2.4.2.). La criminalistique présente les principales disciplines suivantes :

- Preuve biologique - Acide désoxyribonucléique (ADN), fluides corporels, cheveux, tissu, etc.
- Marques – marques sur les doigts et les paumes, marques d'instrument, marques de chaussures, marques de pneus, etc.
- Armes à feu et balistique
- Preuve à l'état de trace – peinture, verre, fibres, explosifs, etc.
- Preuves numériques et électroniques – accès à dispositif, téléchargements de données, analyse, reconstruction de dommages, etc.
- Drogues – identification et quantification
- Analyse de document

[10] Forensic Biometrics: from two communities to one discipline. Proceedings of the International Conference of the Biometrics Special Interest Group 2012 Sept 6-7; Darmstadt, Allemagne.

[11] Nombre sont décrites en détails dans deux publications disponibles auprès de l'Office des Nations Unies contre la drogue et le crime (ONUDC) : 'Police: Forensic services and infrastructure' et 'Staff skill requirements and equipment recommendations for forensic science laboratories'. (www.unodc.org)

- Analyse d'explosif

Le matériel biométrique criminalistique est employé dans les enquêtes pour les comparaisons 1:1 (ainsi la comparaison d'une marque de doigt récupérée sur le lieu d'un crime avec un jeu d'empreintes digitales obtenu d'un suspect) et forme aussi l'un des trois principaux types de bases de données employées par les experts en criminalistique [12]:

1. *Bases de données de référence de matériels d'enquête* – ainsi une collection de fibres naturelles et fabriquées par l'homme, provenant habituellement de fabricants et de détaillants, pour les identifier, les catégoriser et les comparer avec des fibres provenant de scènes de crimes.
2. *Bases de données de recherche non biométriques* – ainsi les armes à feu, munitions, empreintes de chaussures, etc.
3. *Bases de données de recherche biométriques* – collection de caractéristiques et de matériels biologiques humains, ainsi l'ADN et les empreintes digitales.

Les principes de base de la gestion de la preuve en criminalistique doivent être respectés lors du traitement des échantillons biométriques dans le contexte de la criminalistique et des enquêtes. Dans le cas contraire, les résultats produits par un quelconque système de recherche biométrique seront dépourvus de valeur dans le cadre de toute procédure judiciaire ultérieure. Les procédures et enregistrements suivants doivent donc être employés avec constance pour le prélèvement de chaque échantillon /élément d'une scène de crime :

- *Provenance* – un enregistrement textuel et photographique de l'emplacement de l'échantillon /élément
- *Préservation* – l'échantillon /élément criminalistique doit être prélevé et conditionné de sorte que la preuve ne soit pas contaminée, détruite, altérée, perdue ou dégradée. Le conditionnement doit aussi protéger l'échantillon de tout dommage durant le transit et empêcher tout contamination croisée avec d'autres éléments ou environnements. L'échantillon devrait être stocké à une température appropriée pour le préserver et assurer son arrivée dans un état de test optimum pour l'analyse en laboratoire.
- *Intégrité* – le conditionnement doit être robuste, intact et scellé efficacement pour empêcher tout accès sans autorisation ou interférence. Il ne devrait pas être possible d'ajouter ou de retirer du matériel (notamment des particulats, gaz ou liquides) à travers le conditionnement.
- *Continuité (Chaîne de contrôle)* – un enregistrement doit être conservé - à partir de la scène du crime - de chaque personne prenant possession de l'échantillon /élément conditionné.

Étude de cas 2 – L'Innocence Project

L'Innocence Project a été fondé en 1992 par Paul Neufeld et Barry Sheck de la Benjamin N. Cardozo School of Law, New York, États-Unis. Ce projet a pour objectif d'utiliser le profilage ADN criminalistique afin de disculper les individus condamnés à tort et de réformer le système judiciaire criminel américain pour éviter les injustices futures. Le concept reposait sur le principe que si la technologie ADN pouvait prouver la culpabilité criminelle des personnes, elle pouvait aussi disculper

[12] Les bases de données de renseignement criminalistique sont souvent gérées et exploitées par des experts en criminalistique, s'appuyant sur des laboratoires criminalistiques. Toutefois, certaines bases de données biométriques, ainsi les systèmes d'empreintes digitales, d'ADN, vocaux ou faciaux, peuvent être exploitées dans les environnements de maintien de l'ordre par d'autres personnels.

les innocents condamnés à tort. À ce jour, les tests ADN ont abouti à 356 exonérations et à l'identification de 153 coupables alternatifs potentiels.

1.2.1 Bases de données biométriques criminalistiques : Catégories de données

Les bases de données biométriques criminalistiques, aussi dénommées bases de données de renseignement criminalistique, sont employées de manière routinière par les laboratoires criminalistiques et les organismes de maintien de l'ordre. Ces bases de données revêtent un impact significatif sur les enquêtes criminelles, particulièrement sur les cas de terrorisme, dans nombre de pays depuis plus d'un siècle. Parmi les modalités les plus communément utilisées, nous relevons les empreintes digitales, l'ADN, le visage et la voix. Chaque base de données comprend deux ensembles de données distincts :

Données de référence – prélevées sous des conditions contrôlées sur des individus arrêtés ou soupçonnés de délit, ainsi les empreintes digitales des 10 doigts des mains capturées électroniquement avec un scanner ou par des méthodes traditionnelles avec de l'encre et du papier, les frottis buccaux prélevés à l'intérieur de la joue d'un prévenu ou un cheveux, voire un échantillon sanguin, traité afin de générer un profil ADN complet[13], des photographies numériques du visage, etc. Les données de référence peuvent aussi être obtenues des officiers de police et des personnes ayant eu un accès légitime aux scènes de crime, afin d'identifier un quelconque matériel criminalistique déposé par eux et de l'éliminer de l'enquête.

Données de scène de crime – générées à partir d'échantillons et d'éléments prélevés sur les scènes de crime.[14] La qualité des données biométriques de scène de crime peut varier grandement. Un matériel criminalistique récupéré peut être endommagé, contaminé ou manquer de contenu ou de clarté des détails pour une diversité de raisons. De là un large éventail incrémentiel de résultats issus du processus de recherche et de comparaison au lieu d'un résultat binaire correspondance /défaut de correspondance provenant d'autres systèmes biométriques non criminalistiques, ainsi les applications de contrôle d'accès.

Certains pays emploient aussi de grands systèmes biométriques au service de registre de l'état civil de leurs citoyens, comme les programmes de carte d'identité. Chaque citoyen dispose dès lors d'une identité formelle pour accéder aux services publics et autres facilités des secteurs social et commercial, notamment l'État providence, le logement, l'assurance, la banque, etc.

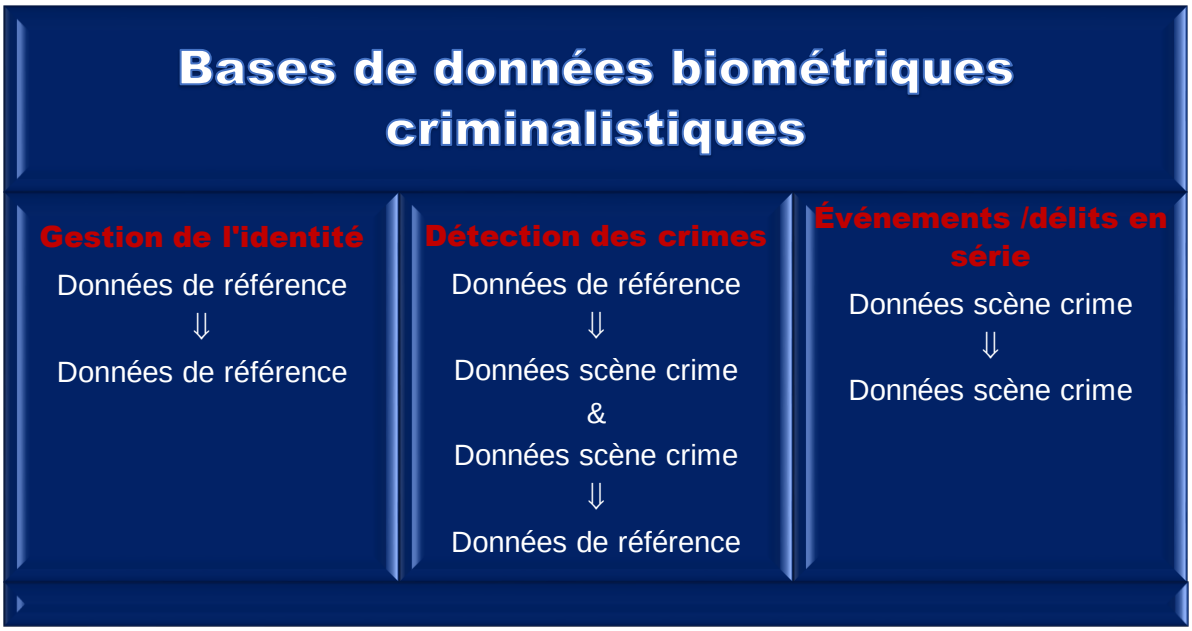
Systèmes de registre d'état civil – Les modalités employées dans ces systèmes sont habituellement les empreintes digitales, le visage ou l'iris, voire une combinaison multimodale. Ces bases de données peuvent contenir des millions ou même des dizaines, voire des centaines, de millions de modèles biométriques (données de référence) selon la taille de la population nationale et sont pensés principalement à des fins de recherche de données de référence. Dès lors, si le système national légal et réglementaire permet aux organismes de maintien de l'ordre d'interroger ces bases de données à des fins d'enquêtes criminelles, les recherches pourraient normalement être limitées aux seules

[13] La technologie ADN moderne assure un profilage rapide des frottis buccaux d'ADN prélevés sur des personnes et exécutés dans des dispositifs complètement automatisés, en laboratoire ou au poste de police /douane, aujourd'hui en à peine plus d'une heure. En d'autres termes, les recherches de base de données ADN peuvent établir une correspondance ADN avec des échantillons de la scène du crime alors que la personne est encore détenue ou en garde à vue.
[14] L'expression 'Scène de crime' est employée ici au sens large pour inclure les emplacements physiques, suspects, victimes, témoins et environnements numériques et électroniques.

données de référence. Il serait possible de rechercher le jeu d'empreintes digitales ou l'image faciale d'une personne afin de s'assurer qu'elle est enregistrée dans le système mais il est peu probable qu'une recherche de marque de doigt ou de visage pour une scène de crime génère une correspondance. Cela tient au fait que les algorithmes de correspondance ne seraient pas normalement conçus pour gérer des données de scène de crime de la même manière qu'un système de recherche criminalistique dans le cadre d'un laboratoire criminalistique. C'est pourquoi les bases de données biométriques civiles sont rarement exploitées dans les enquêtes criminelles et, même lorsqu'elles le sont pour les crimes graves et le terrorisme, le taux de succès est souvent extrêmement bas. Cependant, les nouvelles technologies et sources de données pour certaines modalités, ainsi le visage, pourraient rendre les recherches plus exactes à l'avenir. Nous relevons aussi l'option d'intégration ou de liaison d'un logiciel de correspondance criminalistique avec ces systèmes de registre d'état civil.

1.2.2 Bases de données biométriques criminalistiques : Catégories de recherche

Figure 2 – Bases de données biométriques criminalistiques – Permutations de recherche



Nous comptons quatre permutations de recherche criminalistique basiques employées au service des forces de l'ordre et des enquêtes criminelles, assurées grâce aux trois configurations de recherche suivantes (voir Figure 2) :

Recherche de gestion de l'identité *Permutation 1* - Données de référence avec données de référence

Ce type de recherche détermine si un sujet est déjà inscrit dans une base de données en recherchant ses données de référence en fonction de toutes les données de référence renseignées dans la base de données. Cette technique est le plus souvent utilisée pour établir si une personne est connue de la police et a des antécédents ou un casier judiciaire, spécialement si elle a effectué de fausses déclarations. Ce sont historiquement les empreintes digitales qui ont rempli cette fonction. Un jeu

complet de[15] dix empreintes digitales roulées ('Décadactylogrammes') est prélevé sur un prévenu et recherché dans une base de données de décadactylogrammes de délinquants connus. Cette technique est extrêmement exacte (soit un TAA très élevé - voir Section 1.1) si elle est exécutée sur un système AFIS (Automatic Fingerprint Identification System - Système d'identification automatique d'empreintes digitales) moderne et efficient avec une base de données contenant des images d'empreintes digitales de qualité supérieure, soit des empreintes digitales dont la qualité est assurée et prélevées dans des conditions contrôlées par des opérateurs compétents. Ces recherches sont régulièrement menées de manière 'autonome', soit avec pas ou peu d'intervention humaine sauf si la vérification d'une correspondance est nécessaire. En d'autres termes, ces recherches offrent un traitement extrêmement rapide. Grâce aux dispositifs de capture de données mobiles modernes, les forces de l'ordre peuvent recueillir des empreintes digitales et palmaires sur des personnes se trouvant sur des sites distants, notamment des postes de frontières, et envoyer les données à un serveur central pour une recherche immédiate. Le résultat est normalement reçu en l'espace de quelques secondes ou minutes. Certains dispositifs mobiles intègrent une base de données autonome de sorte que toutes les fonctions de recherche puissent se dérouler localement sans devoir transmettre les données à un serveur distant.

Bien entendu, il est aussi possible de mener une recherche de gestion de l'identité selon d'autres modalités biométriques, ainsi l'ADN, le visage, l'iris, etc. Les recherches de gestion de l'identité peuvent aussi servir à identifier les personnes décédées ou amnésiques. L'impératif clé sous-tendant toute recherche biométrique tient à l'obtention de données de référence de qualité supérieure selon une norme cohérente. De la sorte, toutes les configurations de recherche opèrent à leur potentiel maximum. Un matériel de référence de qualité insatisfaisante compromet l'efficacité et l'exactitude de toutes les permutations de recherche.[16]

Une recherche de gestion de l'identité pose la question : « Nous avons-vous déjà trouvé avant et qui êtes-vous ? ».

Recherche de détection des crimes : *Permutation 2* - Données de référence à données de scène de crime & *Permutation 3* - Données de scène de crime à données de référence

Ce protocole de recherche exige une interface bidirectionnelle entre la Base de données de référence et la Base de données de scène de crime, contenant du matériel biométrique criminalistique prélevé sur des scènes de crime, soit des taches criminelles d'ADN (échantillons interrogés), marques de doigt et de paume, images faciales, etc. Les données de référence nouvellement enregistrées, si elles ne sont pas déjà dans la base de données de référence, sont interrogées dans la base de données de

[15] Le bout de chaque doigt est roulé sur la platine du scanner ou sur le formulaire d'empreinte digitale, d'un bord d'ongle à l'autre, pour enregistrer le maximum de flux de crêtes papillaires et de détails caractéristiques. Les autres impressions des doigts sont connues comme des impressions à plat. Elles sont prélevées simultanément (deux pouces ensemble et les quatre doigts de chaque main) en appuyant le doigt directement vers le bas sur la platine ou le formulaire. Les impressions à plat constituent une mesure d'assurance qualité pour s'assurer que les empreintes roulées ont été enregistrées selon la séquence correcte.

[16] C'est pourquoi, pour toutes les personnes détenues au RU en raison de délits liés au terrorisme, un minimum de trois jeux d'empreintes digitales et palmaires sont prélevés dans le cadre d'une procédure supervisée par un expert en empreintes digitales. Chaque jeu inclut toutes les zones de détail des crêtes papillaires présentes sur la main, soit les impressions à plat et roulées standard, les pointes de doigt, les impressions roulées de toutes les phalanges, la surface intégrale de la paume et le bord ulnaire de la main (paume d'écriture) ainsi que les impressions plantaires (plante des pieds et orteils). Ce processus méticuleux produit les meilleurs jeux d'empreintes digitales de référence pour une recherche AFIS et à des fins d'archivage mais aussi le plus grand ensemble de données disponible des détails de crêtes papillaires par friction pour une comparaison 1:1 avec des marques de doigt /paume /plante de pied d'une scène de crime, spécialement celles des pointes ou des bords de doigt ou toute zone de la paume.

scène de crime et, inversement, les données de scène de crime nouvellement enregistrées sont recherchées dans la base de données de référence. L'exactitude de ces types de recherche peut s'avérer considérablement inférieure à celle d'une recherche de gestion de l'identité en raison de la qualité variable des données de scène de crime.

Une Recherche de détection des crimes pose les questions : « Avez-vous commis un crime ? », « Êtes-vous lié à cet objet /lieu ? » et « Étiez-vous avec quelqu'un d'autre ? ».

Recherche d'événements /délits en série : *Permutation 4* - Données de scène de crime à Données de scène de crime

Ce type de recherche peut relier des scènes de crime de délits distincts ou pouvant se produire dans le cadre d'une grande enquête unique en identifiant et en associant du matériel de scène de crime de différents lieux et en procurant une piste de renseignement aux enquêteurs de ces cas. L'identité de la personne déposant le matériel de scène de crime est inconnue mais le fait de déterminer que la même personne a laissé du matériel biométrique dans le cadre de plusieurs délits ou incidents se révèle une aide précieuse pour les enquêteurs et les analystes du renseignement. La réussite et l'exactitude de ce type de recherche dépendent grandement de la qualité des données de scène de crime et du prélèvement de matériel compatible sur les scènes de crime. Certaines modalités sont mieux adaptées à ce type de recherche que d'autres, ainsi l'ADN est particulièrement efficace pour relier les crimes /événements de différents types d'enquête comme pour le terrorisme, les homicides et les délits sexuels.

Une Recherche de délits en série pose la question : « Ces données de scène de crime correspondent-elles à celles d'autres délits /incidents ? ».

NB Les bases de données décrites dans cette section affichent toutes des taux de rejet faux différents selon le type et la qualité des données biométriques qu'elles contiennent. Comme pour tous les autres systèmes biométriques, un défaut de correspondance ou un résultat négatif (soit une recherche 1:n ne génère aucune correspondance) n'implique pas nécessairement que les données correspondantes ne se trouvent pas dans la base de données mais plutôt que le système peut avoir échoué à les identifier, quelle qu'en soit la raison.

ADN[17] – Catégories de recherche additionnelles

Certaines techniques de recherche spécialisées additionnelles sont aussi spécifiques aux échantillons interrogés d'ADN. Les Profils de référence ADN sont générés à partir de zones non-codantes de l'ADN et uniquement employés à des fins d'identification. En effet, ils contiennent très peu d'autres informations génétiques. Les Échantillons interrogés d'ADN des scènes de crime contiennent habituellement davantage de matériel génétique. De ce fait, d'autres techniques de profilage et d'extraction d'ADN peuvent être employées au profit des enquêteurs. Toutefois, ces techniques sont habituellement sujettes à une surveillance intense de la part des responsables de la supervision juridique et éthique en criminalistique car elles risquent d'enfreindre la législation relative à la vie privée et à la protection des données en l'absence d'une gouvernance rigoureuse. Les exemples incluent :

Évaluation phénotypique – Une technique recherchant des traits physiques génétiques spécifiques comme les cheveux roux ou la couleur des yeux dans une tache criminelle. Bien que ce processus soit actuellement plutôt limité, les avancées de la science ADN vont indubitablement ouvrir l'éventail des

[17] Voir aussi « DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017 » http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

caractéristiques phénotypiques à l'avenir. Potentiellement, les enquêteurs pourraient extraire une 'description' plus détaillée du suspect inconnu à partir de l'ADN d'une tache criminelle.

Recherche familiale (parenté) – Le profil ADN généré à partir d'une tache criminelle peut ne pas être identifié lors d'une recherche dans une Bases de données de référence d'ADN de criminels. Sous des circonstances exceptionnelles, le profil peut être recherché dans la même base de données en employant un logiciel spécialisé additionnel afin de déterminer s'il correspond vaguement à celui d'un ou de plusieurs proches (liens du sang) qui peuvent être enregistrés dans le système. De là relativement peu de réponses générées ou, au contraire, des milliers selon la rareté comparative du profil ADN interrogé par comparaison avec le profil génétique global de la population de la base de données.

1.2.3 Bases de données biométriques criminalistiques – Limitations et normes de signalement

Le matériel criminalistique est habituellement déposé ou enregistré par inadvertance durant la préparation ou la perpétration d'un crime et peut être sujet à une palette de conditions dommageables et de contraintes qui l'empêchent d'être employé avec la même efficience que les Données de référence d'un système de recherche biométrique. Certaines de ces conditions sont de nature générique mais nombre d'entre elles dépendent de la modalité de l'échantillon. Certains exemples communément rencontrés incluent :

Visage – vidéosurveillance et autre technologie d'enregistrement visuel externe

- *Compatibilité d'angle de caméra* – Les caméras de vidéosurveillance se trouvent souvent en hauteur alors que les images d'identité judiciaire sont prises de face et au niveau du visage. La comparaison exacte de ces deux types d'image s'avère donc difficile, voire impossible parfois.
- *Éclairage et exposition* – afin de produire la meilleure image de caméra, les capteurs dépendent (a) de l'éclairage d'ensemble disponible dans un environnement et (b) des réglages comme la vitesse d'obturation, le diaphragme et l'ISO.
- *Résolution de caméra* – certaines caméras affichent une résolution basse et enregistrent donc uniquement un nombre limité de pixels. Si la caméra est à une certaine distance du sujet, l'image résultante est donc souvent granuleuse et indistincte, particulièrement si l'éclairage ambiant est déficient. De là une image contenant peu de détails exploitables, même après agrandissement.
- *Compression* – le composant d'enregistrement des données de la caméra élimine des détails fins afin d'accroître la capacité de stockage des images de définition inférieure.
- *Caractéristiques faciales et masquages* – Des facteurs, comme l'âge, l'expression ou les caractéristiques faciales, qui ne sont pas distinctifs peuvent compromettre la capacité d'identification des visages, tout comme les obstructions externes ainsi les lunettes, pilosités faciales, chapeaux, casques, etc. (voir Section 2.3.2.).

Marques de doigt ou paume (aussi dénommées empreintes latentes ou 'traces') :

- *Caractère suffisant et zone dévoilée* – seule une faible surface du doigt ou de la paume entre en contact avec une surface et donc relativement peu de détails caractéristiques sont révélés.

Les empreintes digitales de référence mal prélevées peuvent aussi contribuer au problème car elles risquent de ne pas révéler cette même petite zone du doigt pour sa comparaison avec la marque de doigt.

- *Surimpression* – plusieurs marques de doigt déposées au même endroit sur une surface rendant difficile l'isolation visuelle d'une impression par rapport aux autres.
- *Interférence* – une interférence contextuelle du substrat peut obscurcir la marque de doigt, en tout ou partie. En général, les marques de doigt sont habituellement soit sur une surface lorsqu'elles sont déposées sur un substrat non poreux, soit absorbées dans la surface d'un substrat poreux. Celles sur la surface sont donc exposées aux dommages et abus environnementaux. La saleté, les contaminants ou autres artefacts peuvent aussi obscurcir ou endommager des détails caractéristiques de la marque.
- *Pression* – le doigt peut être soumis à une pression verticale ou latérale en entrant en contact avec une surface, ce qui peut déformer la marque de doigt du fait de l'élasticité de la peau.
- *Mouvement* – le doigt peut glisser latéralement durant le contact avec une surface, entraînant une impression bavée ou, dans certains cas, une distorsion et une surimpression.
- *Limitations de technique de développement* - l'application de traitements chimiques ou de poudres de développement d'empreinte digitale risque de ne pas révéler toute la marque clairement et peut générer une image trop ténue ou obscure avec peu de contraste.

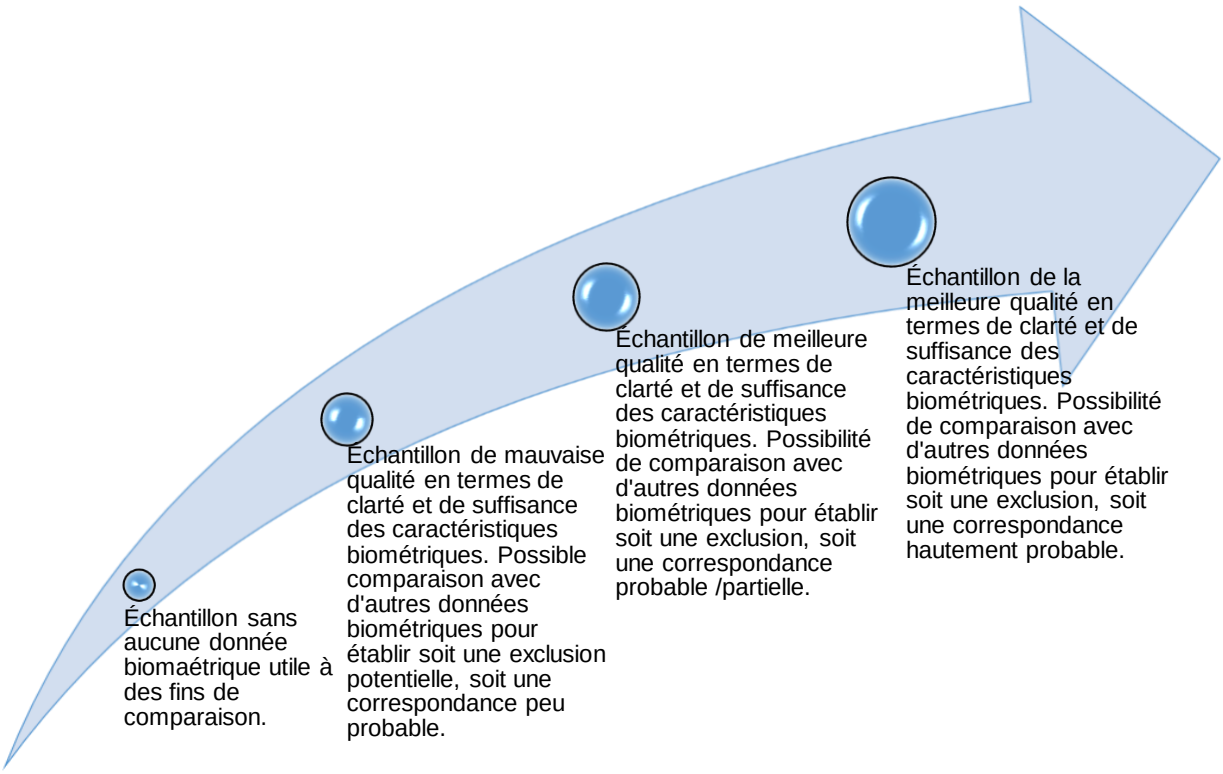
ADN – matériel biologique et cellulaire récupéré des scènes de crime (aussi dénommé 'taches criminelles') :

- *Quantité et qualité* – Comme pour les marques de doigt, la quantité et la qualité de l'ADN déposé sur les scènes de crime sont variables. C'est pourquoi certaines correspondances d'ADN sont classifiées comme 'partielles' et non pas 'intégrales'. C'est le cas lorsque le matériel ADN disponible est insuffisant ou d'une qualité incorrecte afin de produire un profil ADN intégral. Dans ces circonstances, la probabilité de correspondance (ou taux de probabilité) est ajustée en conséquence afin de refléter le degré d'incertitude.
- *Mélanges* – L'ADN de plusieurs donneurs peut se déposer sur le site et le profil en résultant contenir un mélange de plusieurs personnes. Les experts en criminalistique emploient l'analyse statistique pour l'interprétation de ces résultats et, si possible, contribuent à séparer et profiler l'ADN de chaque donneur. Les profils individuels dans le mélange peuvent aussi être de qualité variable.
- *Provenance* – les techniques de laboratoire ADN modernes génèrent des profils à partir de quantités infimes d'ADN au niveau cellulaire. Cependant, comme les scientifiques traitent désormais des échantillons aussi infimes, il n'est pas toujours possible de déterminer la provenance de l'ADN trouvé sur une scène de crime, par ex. un fluide corporel spécifique.
- *Contamination* – cette capacité à détecter et profiler des échantillons ADN aussi infimes a pour conséquence un matériel fugace par nature, soit susceptible d'être transféré entre les personnes, les éléments et les lieux. Des mesures de protection complètes doivent être employées sur les scènes de crime et en laboratoire afin d'éradiquer le transfert par inadvertance d'ADN du fait des actions de la police ou des experts en criminalistique (voir Section 2.3).
- *Abus environnemental* – l'ADN peut être détruit, dégradé ou dénaturé par une exposition prolongée à des conditions environnementales contraires, ainsi des extrêmes de température, humidité et polluants.

Par conséquent, la qualité du matériel biométrique récupéré des scènes de crime s'échelonne progressivement d'une valeur nulle, pour laquelle aucune donnée ou caractéristique biométrique ne peut être extraite, à maximale, soit le matériel biométrique offre une quantité et une clarté suffisantes des caractéristiques pour autoriser une comparaison avec d'autres données biométriques et donc le potentiel de production d'une correspondance hautement probable. La qualité relative des autres données biométriques employées dans la comparaison, soit un échantillon de référence ou un échantillon de scène de crime, est aussi essentielle pour le processus. La capacité à obtenir un quelconque degré de correspondance du processus de comparaison est directement liée à la qualité des deux échantillons. C'est pourquoi les données de référence biométriques prélevées sur des individus en connexion avec des actes de terrorisme doivent être de la meilleure qualité possible.

La Figure 3 illustre les phases représentatives de cette variation en termes de qualité de l'échantillon biométrique et du continuum correspondant, allant des correspondances à probabilité faible à élevée. Les exclusions, la comparaison indiquant que les deux échantillons biométriques n'ont pas été produits par la même personne, sont normalement plus aisées à établir avec des éléments biométriques de qualité inférieure plutôt que les inclusions (soit les correspondances). Cependant, dans la partie basse du continuum qualitatif, les deux processus peuvent s'avérer ardus et les résultats des comparaisons non concluants.

Figure 3 – Données biométriques de scène de crime – La relation entre la qualité de l'échantillon biométrique et les probabilités de correspondance



Critères d'enregistrement de base de données - Des données biométriques de mauvaise qualité manquent habituellement des caractéristiques suffisantes pour une recherche discriminante. En d'autres termes, les données une fois enregistrées sur un système de type AFIS devraient répondre sur une base fréquente et disproportionnée aux recherches, ce qui risquerait de compromettre in fine l'efficacité du système. Cet état de fait est inhérent à la présentation des correspondances biométriques potentielles sous la forme de liste hiérarchisée de candidats, offrant habituellement un nombre prédéfini de réponses, soit les dix correspondances les plus probables. Elles sont vérifiées par un opérateur humain qui détermine si l'une d'elles correspond effectivement. Toutes les données de mauvaise qualité enregistrées dans le système risquent potentiellement d'exclure les correspondances authentiques hors de cette liste. Dès lors, la décision d'enregistrement d'un échantillon biométrique doit être le fruit d'un bilan entre la valeur probante, opérationnelle et de renseignement de chaque échantillon et sa qualité technique ou scientifique (voir Section 2.4.2.). Dans un réseau de bases de données, ces seuils d'enregistrement de données biométriques de mauvaise qualité doivent être soumis à des normes collectives minimum pour assurer une exploitation équilibrée et fluide dans le réseau tout en évitant que les partenaires n'enregistrent des données susceptibles de minorer l'efficience des recherches.

En résultante directe du continuum qualitatif des données biométriques de scène de crime, les experts en criminalistique, les praticiens des empreintes digitales et quiconque traitant du matériel criminalistique ont développé une pluralité de méthodes différentes afin de présenter l'éventail des

résultats de leurs comparaisons aux enquêteurs, analystes du renseignement ou tribunaux. Ces méthodes incluent grossièrement :

- Inférence statistique et probabilité logique 'Bayésienne' de test des hypothèses incluant des taux de probabilité formés sur la base des comparaisons de profils ADN. NB : certains tribunaux et juridictions nationales rejettent certaines variations de ces méthodes statistiques [18]
- Échelles d'équivalence verbale, ainsi les comparaisons d'empreintes digitales modernes et nombre d'autres disciplines criminalistiques
- Conclusions 'absolues', ainsi les comparaisons d'empreintes digitales traditionnelles

En d'autres termes, la méthode de reporting criminalistique *pour la même modalité* peut varier entre les pays, voire les juridictions, selon les exigences respectives en matière scientifique, judiciaire, réglementaire et législative. À son tour, ceci peut affecter non seulement les critères d'enregistrement de chaque base de données mais aussi le type de résultat généré.

Étude de cas 3 – Normes d'empreintes digitales historiques

Certains pays utilisent encore la méthode 'absolue' d'identification des empreintes digitales, soit un système historique reposant sur un processus décisionnel binaire, c'est-à-dire une correspondance ou non, qui exige un nombre minimum prédéterminé de caractéristiques de crêtes papillaires (caractéristiques biométriques) afin de confirmer la correspondance et de présenter la preuve devant le tribunal. Cette norme est inscrite dans la législation judiciaire de certaines juridictions. Toute comparaison d'empreintes digitales ou de marques de doigt présentant un nombre inférieur de caractéristiques de crêtes papillaires à la norme acceptée ne peut dès lors être produite devant le tribunal en tant que preuve. Manifestement, des difficultés pourraient ainsi surgir dans des juridictions opérant selon les principes de divulgation intégrale dans le cadre de leur système judiciaire car un tribunal pourrait exiger d'un expert qu'il donne son opinion sur une comparaison d'empreintes digitales d'intérêt pour le tribunal (soit pouvant peser significativement sur le cas ou s'avérer d'une pertinence particulière pour le dossier du défenseur) mais être jugée par l'expert comme inférieure au seuil de la norme acceptée pour sa présentation au tribunal. Afin de surmonter ces limitations, d'autres pays ont développé et adopté ces dernières décennies une approche holistique non-numérique. Elle n'exige pas un nombre minimum de caractéristiques de crêtes papillaires mais observe plutôt selon trois niveaux distincts les détails des crêtes papillaires de friction dans le cadre d'une évaluation systématique et strictement séquentielle.[19] Cette méthode peut déclarer le résultat d'une comparaison d'empreintes digitales *quelconque* de quatre manières (soit identification, exclusion, insuffisance ou non concluant – ou une terminologie équivalente) et peut donc exprimer un 'degré d'incertitude' conforme avec d'autres disciplines de la criminalistique moderne. Par conséquent, tout échange international de données d'empreintes digitales doit prévoir des tolérances pour ces variations de reporting scientifique des mêmes modalités.

Ce sujet a fait l'objet de recherches et de discussions internationales considérables cette dernière décennie. En effet, nombre de juridictions préféreraient une méthode unique de présentation des résultats scientifiques couvrant les disciplines criminalistiques conventionnelles et les examens criminalistiques associés aux technologies numériques et électroniques. Diverses propositions ont été avancées mais l'accord sur un modèle définitif est encore en souffrance alors que la question

[18] Pour en savoir plus sur ce sujet, voir 'Interpreting Evidence: Evaluating Forensic Science in the Courtroom' de Bernard Robertson & G.A. Vignaux (Wiley ISBN 0471 96026 8, 'Introduction to Statistics for Forensic Scientists' de David Lucy (Wiley ISBN 0-470-02200-0) et 'Strengthening Forensic Science in the United States: A Path Forward' du National Research Council of the National Academies (The National Academies Press ISBN-13: 978-0-309-13135-3).
[19] Cette méthode est connue comme ACE-V (Appréciation, Comparaison, Évaluation et Vérification).

demeure le sujet d'un débat international. Le terrorisme est une menace internationale. Il est donc impératif que les individus traitant des données biométriques et des résultats de recherche soient parfaitement au fait des normes de signalement criminalistique de leurs partenaires nationaux et internationaux pour le partage des données. Une bonne pratique consiste aussi à vérifier tous les résultats produits par d'autres pays partenaires /juridictions en soumettant les correspondances aux protocoles d'analyse criminalistique et aux normes de signalement du pays hôte avant d'entreprendre une quelconque action (voir Section 3.3.3.).

1.2.4 Interprétation scientifique : Identité et activité

Un autre facteur significatif différencie une application biométrique commerciale standard, ainsi un système d'accès biométrique pour un bâtiment, d'une Base de données biométrique criminalistique. Les deux sont capables d'identifier un individu par une recherche 1:1 ou 1:n mais l'application criminalistique offre une capacité additionnelle importante : les données de scène de crime peuvent aussi apporter la preuve d'une activité aussi bien que d'une identité. Le lieu, la position, la distribution et l'orientation d'une preuve criminalistique peuvent être interprétés scientifiquement afin de fournir des informations additionnelles sur le moment et la séquence des événements durant un incident et les activités de ceux impliqués. Cette preuve extra-contextuelle rehausse manifestement la valeur probante du matériel de scène de crime et doit être parfaitement comprise et considérée par les enquêteurs ou analystes gérant les produits des Bases de données biométriques criminalistiques (voir Section 3.3.3.).

NB Les données biographiques et associées recueillies durant les processus de gestion des frontières (voir Section 3.1.1.) peuvent être employées de même, de conserve avec les données biométriques, afin de fournir une preuve d'activité comme d'identité. *C'est l'illustration de l'efficacité de l'exploitation et du partage des données biométriques de frontières comme de scène de crime afin de prédire, suivre et mettre en échec les activités terroristes* (voir Section 3.3.2.1.).

1.3 Pratiques recommandées

a) Les États sont encouragés à adopter ou accentuer leur usage des systèmes biométriques pour authentifier l'identité des individus et les empêcher de fournir de faux renseignements ou de tenter d'usurper l'identité d'autrui.

b) Les systèmes biométriques sont pensés et ajustés selon des besoins d'activités spécifiques en termes d'exactitude, de sécurité, de volumes d'utilisateurs, de rendement et de fiabilité opérationnelle. Les États devraient dès lors évaluer attentivement leurs propres exigences de cas d'usage avant d'investir dans une nouvelle application biométrique.

c) Les processus de Gestion de l'identité biométrique peuvent être rehaussés en les combinant avec des bases de données biométriques criminalistiques afin de créer un cadre de travail efficace d'enquête et de renseignement national pour combattre le terrorisme et les activités criminelles associées.

d) La méthodologie et les normes de signalement criminalistiques internationales présentent des variations. Par conséquent, il est recommandé que l'ensemble du personnel traitant des produits des bases de données biométriques criminalistiques soit formé afin de comprendre la valeur relative et les limitations potentielles des résultats.

1.3.1 Documents de référence

Identity verification- The importance of context and continuity of identity, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

En 1995, la « Biométrie » était définie par le Biometric Consortium du Gouvernement des États-Unis comme « …la reconnaissance automatisée des individus sur la base de leurs caractéristiques comportementales et biologiques ».

Page 1, Biometric Recognition: Challenges and Opportunities, National Research Council, Washington (2010), disponible en téléchargement à :

http://www.nap.edu/openbook.php?record_id=12720&page=1

Jain et al « Biometrics: Personal Identification in Networked Society », Norwell, Mass.: Kluwer Academic Publisher (1999)

Understanding Biometrics Guide (working copy) – Biometrics Institute www.biometricsinstitute.org

PAS 92:2011 Code of Practice for the implementation of a biometric system – British Standards Institute www.bsigroup.com

Office des Nations Unies contre la drogue et le crime (ONUDC) 'Police: Forensic services and infrastructure' et 'Staff skill requirements and equipment recommendations for forensic science laboratories'. www.unodc.org

UK Forensic Science Regulator Annual Report November 2016 - November 2017 – Dr. Gillian Tully

« DNA Database management review and recommendations, 2017, ENSFI DNA Working Group, April 2017 » http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

Forensic DNA Typing: Biology, Technology and Genetics of STR Markers – John M. Butler. Publié par Elsevier Academic Press ISBN-13 : 978-0-12-147952-7

Interpreting Evidence: Evaluating Forensic Science in the Courtroom – Bernard Robertson & G.A. Vignaux. Publié par Wiley ISBN 0471 96026 8

Introduction to Statistics for Forensic Scientists – David Lucy. Publié par Wiley ISBN 0-470-02200-0

Strengthening Forensic Science in the United States: A Path Forward by the National Research Council of the National Academies. Publié par The National Academies Press ISBN-13: 978-0-309-13135-3.

2. Gouvernance et réglementation

À des fins de clarté et de cohérence, la section suivante relative à la gouvernance et à la réglementation concerne toutes les sections de ce compendium et devrait être considérée comme applicable à toutes les pratiques, mesures et recommandations présentées et expliquées dans cette version de ce compendium.

La section 2 traite de la gouvernance et des exigences réglementaires relatives à la technologie biométrique selon les perspectives du droit international, des droits de l'homme, des examens éthiques, des exigences de protection des données et du droit à la vie privée. Elle est suivie par un examen global des vulnérabilités potentielles des systèmes biométriques et de certaines mesures de contrôle servant à atténuer les risques. Les normes opératoires techniques et scientifiques internationales sont ensuite appréciées. Elles couvrent la certification et l'accréditation des applications biométriques mais aussi les systèmes de management de la qualité employés pour les processus criminalistiques associés. La dernière partie de cette section traite des achats, de la maintenance et des exigences de ressources d'un réseau ou d'un système biométrique de lutte contre le terrorisme et, en particulier, des décisions clés elles et financières devant être prises lors de l'évaluation d'un système étendu ou potentiellement nouveau.

2.1 Droit international incluant les droits de l'homme

Les États ont l'obligation de protéger les personnes dans leur juridiction contre les attaques terroristes et de traduire en justice les auteurs de ces actes tout en respectant les droits de l'homme. Le Conseil de sécurité et l'Assemblée Générale des Nations Unies ont souligné que les États doivent assurer que toutes les mesures prises afin de lutter contre le terrorisme respectent l'ensemble de leurs obligations au titre du droit international, en particulier le droit international des droits de l'homme, le droit relatif aux réfugiés et le droit humanitaire. Le respect des droits de l'homme et le régime de l'état de droit sont complémentaires avec les mesures efficaces de lutte contre le terrorisme et essentiels pour le succès de tous les efforts de lutte contre le terrorisme[20].

Il est vrai que la portée d'application des droits de l'homme diffère selon les États membres. Certains États ne sont pas partie des instruments des droits de l'homme universels et nombre relèvent d'instruments des droits de l'homme régionaux[21] qui diffèrent sous certains aspects. Les États membres diffèrent aussi par l'intégration des normes internationales des droits de l'homme dans le droit national. En outre, certains États ont émis des réserves ou des déclarations lors de la ratification ou de l'adhésion, limitant ainsi leur engagement pour des obligations spécifiques des traités.

Dans sa résolution 2396 (2017), le Conseil de sécurité en appelle aux États membres pour apprécier et enquêter sur les combattants terroristes étrangers soupçonnés et les membres de leur famille qui les accompagnent, notamment leurs conjoints et enfants, et pour développer et mettre en œuvre des appréciations du risque complètes pour ces individus. À l'heure du développement de systèmes de collecte des données biométriques, il importe d'instaurer des mesures de protection en regard de la protection des données et des normes des droits de l'homme,[22] en prêtant une attention particulière à la nécessité de s'assurer que tout système conçu pour la collecte et l'enregistrement des

[20] Voir ainsi les résolutions CS 1373(2001), 1624 (2005), 2178 (2014) et 2396 (2017) ainsi que les résolutions AG A/RES/68/276 et A/70/L.55

[21] Voir ainsi la publication de l'Agence des droits fondamentaux de l'Union Européenne 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

[22] S/2015/975, par. 8; S/2015/939, Principe 15 (e).

informations (notamment les données biométriques) concernant des enfants est employé et partagé de manière responsable, protégeant intégralement les droits de l'enfant conformément aux droits national et international, notamment pour les aspects énoncés dans la Convention des Nations Unies relative aux droits de l'enfant (CDE) (1989).

Usage des données biométriques conforme aux droits de l'homme

Les États intègrent de plus en plus l'usage de la biométrie comme un outil important de lutte contre le terrorisme. Identification vocale, scanners de l'iris, reconnaissance faciale, empreintes digitales, ADN, scanners corporels et démarche individuelle : seulement quelques exemples des nombreuses technologies numériques en cours de développement et de déploiement à des fins antiterroristes. Ces mesures technologiques suscitent des défis juridiques et politiques complexes, pertinents pour les efforts des États dans la lutte contre le terrorisme et pour leurs obligations en matière de droits de l'homme. Alors que les systèmes biométriques peuvent être des outils légitimes aux fins de l'identification des terroristes présumés, la portée technique croissante et le développement rapide de cette technologie méritent une vigilance accrue quant à la protection des droits de l'homme, notamment le droit à la vie privée. Le PIDCP 7 stipule que personne ne peut être soumis à une interférence arbitraire ou illégale en regard de sa vie privée, de sa famille, de son foyer ou de sa correspondance, pas plus qu'à des attaques illégales affectant sa réputation ou son honneur et que tout le monde bénéficie de la protection du droit contre ces interférences ou attaques. Le Conseil des droits de l'homme des Nations Unies a reconnu que les « violations ou abus relatifs au droit à la vie privée risquent d'affecter la jouissance d'autres droits de l'homme, notamment le droit à la liberté d'expression et d'opinion sans interférence et le droit à la liberté de réunion et d'association pacifiques.... »[23] Alors que le droit à la vie privée, selon le droit international, n'est pas de nature absolue, il est toutefois reconnu que toute interférence avec le droit doit respecter les principes de légalité, de proportionnalité et de nécessité. Plus loin, une interférence avec la vie privée autorisée par un État peut uniquement se produire sur le fondement du droit, qui doit à son tour respecter les dispositions, buts et objectifs du Pacte et s'avérer raisonnable dans les circonstances du cas.[24]. Toute interférence de la sorte ne doit pas non plus constituer une discrimination au motif de la race, de la religion, de l'origine nationale ou sociale, des opinions politiques ou autres et de quelque autre motif établi par le droit international.[25]

Le Rapporteur spécial des Nations Unies sur le droit à la vie privée a noté que nombre de pays dans le monde ont identifié un droit fondamental primordial à la dignité et au développement libre et sans entraves de la personnalité de chacun, susceptible d'être amoindri par des violations du droit à la vie privée.[26] La Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques commencent par une reconnaissance de la dignité inhérente et des droits égaux et inaliénables de tous les membres de la famille humaine en tant que fondations de la liberté, de la justice et de la paix dans le monde.[27] Ces droits pourraient être compromis par un usage inapproprié des données biométriques. L'abus de ces données pourrait aussi faire peser des risques graves sur le respect des droits de la défense, notamment la présomption d'innocence et d'autres droits connexes avec les poursuites pénales.[28] En outre, la collecte en masse de ces données sans respecter les principes de nécessité et de proportionnalité pourrait constituer en elle-même une violation du droit à la vie privée.[29]

---

[23] Résolution du Conseil des droits de l'homme A/HRC/RES/34/7 (2017).
[24] Commentaire général du Comité des droits de l'homme Nº 16 : Article 17 (Droit à la vie privée), par. 3-4.
[25] PIDCP, Art. 2(1) et 26.
[26] Rapport du Rapporteur spécial sur le droit à la vie privée, A/HRC/31/64 (2016).
[27] Déclaration universelle des droits de l'homme et PIDCP, préambule.
[28] PIDCP, Art. 9 et 14.
[29] PIDCP, Art. 2(3).

Pour éviter un usage inapproprié des données biométriques, les États devraient envisager l'examen de leur législation concernant la protection des données à caractère personnel en l'ajustant pour respecter les applications actuelles des technologies biométriques améliorées. Les États devraient aussi évaluer leur législation pour relever les défis issus du développement plus avant des technologies biométriques. Une approche reposant sur les droits de l'homme de l'usage de la technologie biométrique devrait inclure le recours à des mesures de protection procédurales et à une surveillance efficace de son application.[30] Il s'agit là d'établir des organismes de surveillance appropriés et indépendants afin de superviser les activités des organismes publics, chargés de proposer des recours efficaces en cas de violations, et de créer des autorités de supervision indépendantes pour assurer la conformité des organismes publics et du secteur privé avec le droit relatif à la vie privée et à la protection des données.[31].

2.1.1 Éthique et biométrie

Les technologies comme la biométrie engendrent des défis particuliers en raison du fossé créé entre l'innovation technologique et l'entrée en vigueur de la législation d'encadrement de ces technologies. Par conséquent, certains États ont lancé un examen éthique ou créé des organismes de supervision afin d'anticiper et d'évaluer ces nouvelles techniques ou applications et d'offrir des conseils sur les législations, politique gouvernementales et planification stratégique actuelles et potentielles. Ces instances comprennent habituellement des professionnels chevronnés et experts de l'ensemble de la société civile et peuvent inclure des membres des secteurs public et privé, des sphères scientifique et technologique mais aussi des universitaires et des profanes. Ces groupes de supervision éthique tentent d'examiner les questions selon une perspective étendue incluant l'impact potentiel des technologies biométriques sur certains groupes de personnes ou communautés, particulièrement en termes de race, genre, âge, croyances religieuses et orientation sexuelle.

L'étude de cas suivante illustre cette approche :

[30] Le Comité des droits de l'homme, dans son commentaire général Nº 16 (1988), a mis en exergue le fait que les États devraient prendre des mesures efficaces pour assurer que les informations concernant la vie privée d'un individu ne tombaient pas entre les mains de personnes qui ne seraient pas autorisées par la loi à les recevoir, traiter et utiliser, et qu'elles ne seraient jamais employées à des fins incompatibles avec le Pacte international relatif aux droits civils et politiques. Une protection efficace devrait inclure la capacité pour chaque individu de déterminer sous une forme intelligible l'éventualité, la nature et les fins du stockage de données à caractère personnel sous forme de fichiers de données automatisés, avec un droit correspondant à exiger la rectification ou l'élimination des données incorrectes. Chaque individu devrait aussi être en mesure de déterminer les autorités publiques ou les individus et organismes privés contrôlant leurs fichiers ou susceptibles de le faire. Voir :
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

[31] Résolution AG 45/95 (1990) sur les principes directeurs pour la réglementation des fichiers personnels informatisés et Règlement général sur la protection des données de l'Union Européenne de 2018, Article 51 (Autorité de contrôle).

Étude de cas 4 – Le groupe Biometrics and Forensics Ethics du Royaume-Uni[32]

Ce groupe est une émanation du groupe national initial sur l'éthique ADN, créé pour superviser les techniques et tactiques scientifiques employées dans la première base de données d'ADN au monde. Sa mission couvre désormais la criminalistique en général mais aussi la technologie biométrique. Le groupe envisage chaque nouvelle question dans le cadre d'un cadre de travail étendu de considérations juridiques, morales et sociopolitiques. Il œuvre selon les principes directeurs suivants :

Principes directeurs ***Applicables aux procédures biométriques et criminalistiques :***	**Principes directeurs** ***Mise en œuvre des principes***
- les procédures devraient servir à rehausser la sécurité et le bien publics ; - les procédures devraient servir à promouvoir la justice ; - les procédures devraient respecter les droits de l'homme des individus et des groupes ; - les procédures devraient respecter la dignité de tous les individus ; - les procédures devraient, dans la mesure du possible, protéger le droit au respect de la vie privée et familiale s'il n'est pas en conflit avec les buts légitimes du système pénal visant à protéger le public contre tout dommage ; - les développements scientifiques et technologiques devraient être exploités pour promouvoir une disculpation rapide des innocents, assurer la protection et la résolution pour les victimes et contribuer au processus judiciaire ; - les procédures devraient reposer sur des preuves rigoureuses ;	- impartialité – les procédures devraient être appliquées sans parti pris ou discrimination injuste ; - proportionnalité – équilibre des droits individuels et du bien public ; - ouverture et transparence ; - le besoin de systèmes en place pour identifier les erreurs ; - le besoin de contrôle qualité ; - le besoin de responsabilité des autorités publiques ; - le besoin de supervision indépendante si cela s'avère approprié ; - le besoin de fournir des informations adéquates et, si cela s'avère approprié, d'obtenir le consentement des personnes dont les données ou échantillons sont recherchés.

Le groupe a aussi défini un ensemble de principes concernant la collecte et le traitement des données :

- les données devraient être collectées, stockées et utilisées uniquement pour les fins légales spécifiées ;
- la collecte, le stockage et l'utilisation des données doivent respecter les exigences légales ;

[32] https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group

- des mesures devraient être prises pour assurer l'exactitude, la sécurité et l'intégrité des données collectées, stockées et utilisées ;
- les processus devraient être rigoureux, conformes avec les normes internationales et appliqués par un personnel professionnel formé ;
- les intrusions dans la vie privée devraient être minimisées ;
- les intérêts des personnes concernées secondaires (soit les personnes potentiellement affectées par les données collectées sur autrui, notamment les membres de la famille) devraient être pris en compte ;

La menace du terrorisme affecte nombre d'États et, en conséquence, de nouvelles techniques biométriques et criminalistiques sont en voie de développement et de déploiement rapides par les organismes de maintien de l'ordre afin d'assurer la protection et de rehausser les capacités d'enquête. Les groupes de surveillance éthique ont un rôle à jouer dans ce processus car ils sont en position de commenter de manière informée la préparation ou l'adoption d'une quelconque nouvelle technique ou stratégie. Il ne s'agit pas là de remplacer le besoin de législation ultérieure mais d'aider à éviter l'introduction de nouvelles méthodes et pratiques qui ne seraient pas proportionnées, ni même nécessaires. Ce processus alerterait aussi le législateur de l'urgence et de l'importance relative de la question examinée.

Normes et exemples d'interactions de l'éthique et de la biométrie

Actuellement, les normes de délivrance et d'usage éthiques de la biométrie et de la plupart des nouvelles technologies sont hétérogènes aux échelons international et même national. L'ISO (International Organization for Standardization - Organisation internationale de normalisation) a promulgué ses normes relatives aux Considérations juridictionnelles et sociétales pour applications commerciales -- Partie 1: Guidage général (ISO/IEC TR 24714: 2008) et ses Guide 71:2014, qui traite de l'éthique, et 71, comportant les normes d'accessibilité pour les groupes comme les personnes âgées ou handicapées.

L'usage éthique de la biométrie se prolonge jusqu'au domaine de l'humanitaire. De nombreux programmes ont constaté le caractère bénéfique de l'usage de la biométrie. Le bureau du Haut-Commissaire des Nations Unies pour les réfugiés (HCR), par exemple, a employé des systèmes biométriques au service de ses programmes depuis 2002 et fonde toujours plus ses enregistrements sur la biométrie. Grâce à la solution biométrique globale du HCR, le BIMS (Biometric Identity Management System - Système biométrique de gestion de l'identité), l'organisation s'assure du caractère unique de chaque enregistrement et vérifie que les diverses formes d'assistance que l'organisation peut offrir (notamment la nourriture, les espèces, la protection ou les interventions de réinstallation, entre autres) sont reçues par les bénéficiaires légitimes. D'autres exemples portent sur les fraudes électorale et financière, deux facteurs potentiellement déstabilisateurs susceptibles d'encourager la rébellion et la croissance du terrorisme, qui sont minimisées par le recours à l'identification selon la biométrie.

Le HCR recommande aussi l'enregistrement biométrique des demandeurs d'asile comme un élément intégrant des systèmes de saisie sensibles à la protection. Il s'agit notamment là d'instituer des mesures de protection appropriées pour éviter une infiltration possible de criminels ou membres d'organisations terroristes ou extrémistes. À cet égard, les bonnes pratiques incluent : (1) l'enregistrement approprié, notamment la biométrie par les autorités aux frontières formées sur les aspects pertinents de la sécurité, des réfugiés et de protection des droits de l'homme et (2) la référence des personnes prétendant réclamer une protection internationale dans le cadre des

procédures d'asile. Par principe et afin de ne pas exposer les demandeurs d'asile /réfugiés au risque, leurs données biométriques et autres à caractère personnel ne devraient pas être partagées avec leur pays d'origine sauf si la procédure d'asile s'est terminée et la protection n'a pas été accordée. C'est aussi le cas pour les pays tiers dans des circonstances où une protection efficace du demandeur d'asile ou du réfugié pourrait être exposée à un risque.[33]

2.2 Protection des données et droit à la vie privée

La technologie biométrique s'avère un atout significatif pour la lutte contre le terrorisme à l'échelon global. Elle a la capacité de détecter et de mettre en échec les activités terroristes et de protéger la société contre les attaques aveugles. Cependant, la technologie repose sur la collecte, le stockage et l'utilisation des données à caractère personnel. Comme vu auparavant, ces données biométriques doivent être protégées par le droit et traitées sans violation des droits de l'homme fondamentaux, ainsi le droit à la vie privée.

2.2.1 Critères d'enregistrement légal et normes des données

Le Conseil de sécurité des Nations Unies dans sa résolution 1373 (2001) a noté une connexion étroite entre le terrorisme international et les activités transnationales du crime organisé, des drogues illicites, du blanchiment d'argent et du trafic d'armes. Dans cette même résolution, le Conseil a décidé que les États devaient éviter les mouvements des terroristes et groupes terroristes grâce à des contrôles efficaces aux frontières et à des contrôles de la délivrance des documents d'identité et de voyage mais aussi par des mesures destinées à éviter la contrefaçon, la falsification ou l'usage frauduleux de ces documents d'identité et de voyage.

Pour contrecarrer cette relation, il est essentiel de développer une capacité suffisante et efficace de lutte contre le terrorisme entre tous les États membres.[34] L'usage de la biométrie est un outil vital du développement de cette capacité.[35] Comme les tactiques employées par les terroristes incluent souvent le vol de documents ou d'identités, l'usage de la biométrie procure un outil précieux de rétablissement des identités des victimes de vol d'identité (voir Section 2.3.5.).

Pour mettre en œuvre un système biométrique à la fois efficace et conforme avec la législation relative à la protection des données tout en préservant le droit à la vie privée, les facteurs suivants sont à prendre en compte :

Assurance qualité d'enregistrement - des normes de qualité élevées doivent être définies pour les enregistrements de sorte que l'enregistrement et la correspondance biométriques puissent être employés avec exactitude dans une vaste diversité d'environnements, ainsi des sites distants, postes frontières fixes ou aéroports, qui exigent un traitement sans cesse plus rapide des passagers tout en préservant les niveaux d'exactitude. Dans le cas des enfants ou des mineurs juridiques accompagnés de leurs parents ou voyageant seuls, il convient de tenir dûment compte de la possibilité que certains aspects biométriques des enfants peuvent changer à mesure de leur développement. En outre, le Conseil de sécurité des NU dans sa résolution 2396 (2017) souligne que les enfants doivent être

[33] Voir Section E, paragraphe 17 du document du HCR « Appréhender les questions de sécurité sans porter atteinte à la protection des réfugiés »
http://www.refworld.org/docid/5672aed34.html
[34] Voir également les résolutions du Conseil de sécurité 2195 (2014) et 2178 (2014)
[35] Résolution du Conseil de sécurité des NU 2396 (2017) et sa résolution antérieure 2178 (2014)

traités de sorte à respecter leurs droits et leur dignité conformément au droit international applicable.

Législation sur la vie privée - Les autorités de maintien de l'ordre peuvent limiter le droit à la vie privée si les mesures prises s'avèrent nécessaires et proportionnées mais aussi en conformité avec le droit international des droits de l'homme. Par exemple, les données à caractère personnel des suspects et associés peuvent être utilisées en cas d'urgence lorsque les principes clés relatifs à la vie privée, ainsi le consentement informé ou la collecte des données à caractère personnel connexes, peuvent être écartés. Cependant, ces principes relatifs à la vie privée, comme le consentement informé, la collecte et l'usage uniquement aux fins énoncées ainsi que le droit de correction des enregistrements inexacts ou trompeurs, devraient être traités comme des exigences par défaut dans la majorité des cas. En outre, les raisons motivant le non-respect de ces exigences par défaut devraient être documentées et consignées. L'accès des opérateurs à ces systèmes devrait aussi être contrôlé par la biométrie afin d'assurer des normes élevées de sécurité.

Financement du terrorisme - pour contribuer à la prévention des fraudes, vols d'identité et transactions financières connexes au terrorisme, la biométrie peut être employée dans le cadre d'un ensemble de mesures pour atténuer ces menaces à l'échelle du système financier. L'usage de la biométrie pour le contrôle de l'accès aux transactions s'avère donc une option efficace. Un programme à l'échelle de la nation pour la protection des consommateurs contre les vols d'identités et fraudes connexes au terrorisme comporte maints avantages aux niveaux communautaire et policier.[36]

Normes internationales sur les données à caractère personnel - les normes relatives aux données à caractère personnel devraient être définies en conformité avec des normes internationales plutôt qu'en employant des modalités ou normes techniques moins communes, susceptibles de reposer sur des facteurs comme le lobbying sectoriel autochtone ou même des systèmes procurés à titre gratuit des donateurs. Les normes pertinentes de l'Organisation internationale de normalisation (ISO), de l'Organisation de l'aviation civile internationale (OACI) et de l'Organisation mondiale des douanes (OMD) devraient offrir les critères initiaux pour la sélection de système, avec l'assistance des Principes directeurs relatifs à la vie privée et de la Liste de contrôle d'appréciation des répercussions sur la vie privée du Biometrics Institute.[37]

Admissibilité de la preuve - des précautions devraient être prises pour assurer que l'usage de l'ensemble des données à caractère personnel et biométriques soit limité aux fins approuvées pour lesquelles elles ont été obtenues. Elles constitueraient aussi une assurance que les données collectées pour les bases de données sont admissibles à des fins de poursuites judiciaires. Elles devraient inclure des dispositions assurant la coopération du secteur TCI dans la mesure où un fondement juridique a été établi pour une telle coopération.

Interprétation des sorties biométriques – les organismes de maintien de l'ordre qui arrêtent ou entament des poursuites contre les terroristes devraient être conscients des risques d'erreur d'interprétation des résultats des bases de données biométriques, en comprenant la valeur d'une correspondance ADN partielle ou de l'échec d'une comparaison faciale en raison des problèmes environnementaux pouvant se produire lorsqu'une image faciale est capturée dans un environnement de mauvaise qualité. Dans ces cas, une analyse contextuelle est absolument essentielle avant d'entreprendre une quelconque action (voir Section 3).

[36] Voir le site Web du Fonds Monétaire International sur lequel les instruments de lutte contre le blanchiment d'argent et autres fraudes sont listés www.imf.org

[37] Voir www.biometricsinstitute.org

2.2.2 Politique de rétention ou de suppression des données

Il s'agit d'un domaine où les procédures de maintien de l'ordre et de lutte contre le terrorisme doivent respecter le droit international des droits de l'homme, notamment le droit à la vie privée. Par exemple, le droit de consulter son dossier, d'apporter des corrections ou d'exiger des suppressions (souvent garantis dans la législation relative à la vie privée, ainsi le *Règlement général sur la protection des données* - RGPD - de l'Union Européenne)[38] peut aussi être qualifié par le besoin de protéger des témoins ou la confidentialité des enquêtes en cours.

Les politiques de rétention des données varient grandement dans le monde, spécialement pour les personnes arrêtées dans le cadre des enquêtes des forces de l'ordre. Nombre de juridictions conservent les données biométriques des criminels condamnés pendant toute la vie du coupable mais aucune norme commune n'existe pour les personnes soupçonnées ou arrêtées pour des crimes mais sans condamnation par la suite.

Une bonne pratique consiste à stocker les données biométriques séparément des données biographiques connexes. Les victimes de vols d'identité (suite à une activité criminelle ou terroriste) peuvent nécessiter un rétablissement accéléré de leur identité après un vol ou un abus. Pour la conception des systèmes, il s'avère nécessaire de planifier la reconnexion des données biométriques et biographiques lorsque c'est le cas. Il peut suffire d'affecter un segment unique de métadonnées aux enregistrements biométriques sous la forme d'un numéro de référence unique. Cependant, cette reconnexion devrait être protégée pour assurer en permanence l'intégrité des systèmes et des données, et imposer un protocole de sécurité rigoureux, ainsi :

- exigence que le responsable accédant aux données relève d'un niveau hiérarchique supérieur au sein de l'organisation,
- usage de ses données biométriques pour accéder au système,
- enregistrement formel de cet accès et
- enregistrement formel des raisons motivant cet accès.

La sécurité peut encore être rehaussée en impliquant plusieurs personnes de l'organisation dans la validation des entrées ou dans le processus de révocation. Une rotation du personnel assumant ces fonctions deviendrait ainsi possible tout en créant une couche de sécurité additionnelle.

2.2.3 Traitement des données

Une organisation responsable du traitement des données doit nommer un responsable du traitement des données, en charge de la gestion de toutes les activités de traitement des données incluant la collecte, le stockage, l'usage et la suppression des données. Le responsable du traitement des données assume la responsabilité même si la fonction de traitement des données est externalisée à d'autres parties.

La législation relative à la vie privée la plus ambitieuse exige des autorités recueillant des données à caractère personnel qu'elles s'assurent qu'aucun traitement ou stockage des données ne soit possible

[38] Règlement général sur la protection des données de l'Union Européenne de 2018, Article 7 (Consentement), Article 17 (Droit d'effacement) et Article 15 (Droit d'accès aux données)

dans des pays où la législation relative à la vie privée présente un niveau inférieur à celle du pays de collecte.

Tout opérateur ou prestataire tiers devrait être contraint par des contrats exigeant un niveau très élevé de sécurité, impliquant des audits externes par l'organisme mandant ainsi que des pénalités pour défaut de conformité, les exigences de sécurité et de confidentialité figurant au contrat.

2.2.4 Partage de données

Dans nombre de déclarations, les Nations Unies ont mis en exergue la nécessité de coopération entre les États en termes d'améliorations législatives pour les poursuites contre les terroristes, spécialement les combattants terroristes étrangers, tout en préservant simultanément le droit, les droits de l'homme et la vie privée.[39] Le partage en temps réel des données à caractère personnel, ainsi la biométrie, au sein des autorités publiques comme entre États exige aussi la coopération. L'objectif est ici l'harmonisation de l'interopérabilité des plateformes et formats.[40]

Si des données à caractère personnel sur les terroristes, réels ou soupçonnés, sont partagées, une confiance considérable sera nécessaire sur maintes questions comme l'usage concret des données partagées, l'exactitude et le contexte des données ainsi que la quantité et le type de données susceptibles d'être partagées. Les ententes de partage de données devraient être fondées sur des accords formels entre toutes les parties impliquées.

D'autres facteurs doivent être pris en compte pour le processus de partage. Ils incluent un exigence que les demandes de données à caractère personnel reposent sur une suspicion authentique d'activité terroriste, des détails d'exigences probantes et la certitude que les données n'ont pas été obtenues sous des conditions d'oppression - une question probante clé dans nombre de pays.

Généralement, les principes suivants s'appliquent :

1. le partage des données à caractère personnel, notamment la biométrie, doit être approuvé légalement à l'échelon national et soumis à un cadre de travail juridique clair entre les entités émettrices et réceptrices des données, nationalement et internationalement.
2. l'usage de ces données doit être limité aux fins approuvées pour lesquelles elles ont été obtenues.
3. les données peuvent uniquement être partagées avec des bénéficiaires de confiance. [41] Le principe énoncé en Section 2.2.3. s'étend au partage des données et les données à caractère personnel ne devraient pas être envoyées dans des juridictions où le niveau de protection de la vie privée est inférieur à celui du pays émetteur.
4. (selon la Section 2.1.) afin de ne pas exposer les demandeurs d'asile ou réfugiés au risque, leurs données biométriques et autres à caractère personnel ne devraient pas être partagées avec leur pays d'origine sauf si la procédure d'asile s'est terminée et la protection n'a pas été accordée (voir aussi Étude de cas 10).

[39] Résolution du Conseil de sécurité des NU 2322 (2016) relative à la coopération internationale et Résolution du Conseil de sécurité des NU 2396 (2017) de renforcement des mesures de lutte contre les menaces posées par le retour des terroristes étrangers.

[40] Résolution du Conseil de sécurité des NU 2178 (2014) et Déclaration de Madrid des ministres des Affaires étrangères lors de la réunion spéciale du Comité contre le terrorisme du Conseil de sécurité du 28 juillet 2015.

[41] Des exemples de partage de données à caractère personnel entre bénéficiaires de confiance sont les accords entre l'ACRO du Royaume-Uni pour les données d'infraction emportant inscription et le Federal Bureau of Investigation (FBI) des États-Unis, des autorités chargées de la police ou de l'immigration de l'Union Européenne, le système de communications sécurisé entre polices I-24/7 d'INTERPOL sous-tendu par la base de données des Documents de voyage perdus ou volés et les documents de voyage associés au système de notices d'INTERPOL.

2.2.5 Prévention des abus de données

En l'occurrence, au moins deux aspects clés sont liés aux abus de données.

Le premier est l'absolue nécessité de sécuriser toutes les données à caractère personnel, notamment la biométrie, contre tout abus ou accès sans autorisation. Il s'agit là aussi bien des menaces externes que des méfaits internes du personnel autorisé.

Le second est la nécessité d'assurer que les données à caractère personnel procurées sont exactes, contextualisées de manière pertinente et fournies sans intentions malveillantes. Cet aspect est spécialement important si un gouvernement ou une autre partie peut souhaiter placer des opposants politiques sur des listes de surveillance dans l'intention d'affecter leurs droits fondamentaux.

2.2.6 Sécurité et validation des données

Chaque organisation devrait nommer un Responsable du traitement des données affichant une expérience, une formation et une expertise suffisantes pour assumer la responsabilité de la collecte, de l'usage et du mouvement de toutes les données à caractère personnel, notamment biométriques.

Les responsabilités clés de ce rôle devraient couvrir la définition de politique et les procédures opérationnelles normalisées. Le titulaire du rôle devrait aussi décider, durant la phase de conception du système, de la ou des modalités biométriques les plus adaptées à l'application.

Toutes les pratiques et politiques efficaces relatives à la sécurité et à la vie privée exigent, indépendamment de l'usage ou non de la biométrie, au moins la prise des décisions suivantes :

- ☐ Une appréciation des répercussions sur la vie privée[42] a-t-elle été menée avant l'introduction d'une nouvelle pratique ou technologie d'activité ?
- ☐ Existe-t-il des procédures et programmes de formation et de sensibilisation préservant une culture adéquate de la confidentialité et des droits de l'homme mais aussi une connaissance concrète de la biométrie par l'ensemble du personnel d'exploitation du système ?
- ☐ Des techniques de cryptage ou de réduction des données sont-elles employées lors des phases critiques de la collecte, du stockage, de l'usage et du partage des données à caractère personnel, notamment biométriques ?
- ☐ Existe-t-il un contrôle d'accès et une journalisation des accès rigoureux exigeant la présentation de données biométriques par les personnes accédant aux fichiers de données à caractère personnel sensibles ?
- ☐ Existe-t-il des processus documentés définissant les mécanismes de signalement et les actions correctives nécessaires en cas de violations de la vie privée et de la sécurité ?
- ☐ Des tests et audits réguliers sont-ils menés pour assurer le respect des pratiques relatives à la sécurité et à la vie privée qui demeurent rigoureuses et efficaces ?
- ☐ Existe-t-il un processus formel de documentation et de traitement des problèmes devenus manifestes en résultante de l'audit régulier ?

[42] Une Appréciation des répercussions sur la vie privée (ARVP) forme partie d'une approche de 'confidentialité conceptuelle' de la gestion des données au sein des organisations publiques et commerciales. Le processus ARVP assure la conformité avec les exigences juridiques et réglementaires en termes de vie privée par l'identification de risques potentiels et le développement de stratégies d'atténuation pour les gérer.

- Des contrôles réguliers et aléatoires sont-ils menés sur la validité et l'intégrité des données à caractère personnel détenues dans le système ?

Différentes normes et principes directeurs internationaux offrent des conseils aux Responsables du traitement des données et à leurs organisations.[43]

En termes de validation des données collectées, notamment biométriques, il est essentiel que la procédure établie soit respectée afin de protéger les droits de l'homme, notamment le droit à la vie privée, mais aussi pour assurer que les impératifs judiciaires en matière de condamnation ou, par exemple, de procédures d'extradition sont parfaitement respectés. Pour les procédures d'extradition, ces impératifs peuvent être plus exigeants dans certains pays, spécialement en termes de critères probants et d'interrogatoire.

Un principe directeur clé pour les autorités de maintien de l'ordre et de gestion des frontières devrait être l'exigence de disposer d'une équipe dédiée d'analystes bénéficiant des compétences et des ressources pour procurer des résultats actionnables et exacts. Ceci contribue à la surveillance des terroristes avant et après un incident et à l'acquisition de preuves admissibles, notamment de nature biométriques comme l'ADN, les empreintes digitales, le visage et la voix. Cette capacité devrait exploiter pleinement l'ensemble des techniques de capture et de recherche biométriques.

2.2.7 Supervision

Les abus des données à caractère personnel (malveillants ou par erreur) peuvent entraîner des conséquences juridiques néfastes et autres dommages pour les individus. C'est particulièrement le cas des listes de surveillance et autres mécanismes d'alerte.

Des précautions devraient être prises à l'heure de l'inscription de criminels ou terroristes soupçonnés sur des listes de surveillance. Des contrôles rigoureux et scrupuleux devraient être appliqués pour apprécier les raisons de l'inclusion et la validité de toutes les requêtes avant l'inscription des données d'un individu sur la liste. Les données contenues dans les listes de surveillance doivent être soumises à un examen régulier pour s'assurer de leur caractère actualisé et pertinent.

De même, en conformité avec le droit international des droits de l'homme et la législation relative à la vie privée, les personnes concernées devraient disposer d'un droit de révision contre leur inclusion sur une quelconque liste. Le droit de révision et d'appel ainsi que l'existence de mécanismes de réclamation devraient être rendus publics par les autorités en charge des listes.

Durant le processus d'inclusion, les autorités de maintien de l'ordre, de lutte contre le terrorisme et de gestion des frontières ont le devoir légal de collecter, de stocker et d'analyser les données de terroristes soupçonnés et de leurs associés ainsi que les modèles comportementaux comme les itinéraires de vol, transactions financières et changements de domicile. Cependant, il convient de s'assurer que les informations sur les suspects et leurs associés demeurent confidentielles et respectent le cadre juridique autorisé de sorte à éviter toute séquestration ou persécution.

Des mesures de protection solides doivent être prévues contre la collecte, le stockage et l'usage arbitraires des données à caractère personnel, notamment des mécanismes de supervision par un

[43] Résolution AG 45/95 (1990) sur les principes directeurs pour la réglementation des fichiers personnels informatisés et *Principes directeurs en biométrie* du Biometrics Institute pour un usage international www.biometricsinstitute.org

organisme indépendant. Il est possible que les États comptent déjà sur des organismes de supervision en charge de la vie privée, capables d'assumer cette fonction dans le cadre de leurs missions existantes ou accrues. Cependant, si un État ne dispose pas encore d'un tel organisme, il devrait en créer un afin d'assumer ce rôle vital.

En particulier, il est essentiel de disposer de mécanismes de supervision définis par le droit qui soient indépendants, efficaces et impartiaux. Ils devraient disposer de pouvoirs de surveillance et d'appréciation de l'adéquation des mesures de protection des données biométriques, notamment en termes de partage international de telles données. Les individus devraient pouvoir contacter le mécanisme de supervision à des fins d'information sur leurs données et de dépôt de plainte s'ils estiment que leurs droits sont en péril. Dans la mesure du possible, les informations sur la gestion de leurs données devraient être procurées sous une forme claire et simplifiée aux personnes concernées. Des recours adéquats devraient être prévus par la loi pour les violations des droits de l'homme inhérentes à la gestion des données biométriques, notamment des violations du droit à la vie privée.

2.3 Gestion du risque système

La gestion du risque système implique le catalogage des défaillances du système, soit pour une partie (ainsi un lecteur de données biométriques), soit dans son intégralité (la configuration du système) et la détermination de la probabilité que ces défaillances entraînent un risque de dysfonctionnement du système. Elle identifie les menaces et les risques puis analyse les conséquences de la réalisation ou de l'exploitation d'une menace et met enfin en œuvre des mesures d'atténuation, si nécessaires.

Les systèmes biométriques impliqués dans les applications de lutte contre le terrorisme sont habituellement complexes, impliquant de multiples composants IT, des interactions avec l'environnement d'acquisition et une interprétation humaine. De là une situation de risque polyfacétique démultipliant les points de défaillance potentiels, spécialement du fait que les cibles terroristes sont hautement motivées et disposent souvent d'excellentes ressources pour contourner les contrôles de sécurité.

La mise en œuvre des systèmes de lutte contre le terrorisme sans l'application de la gestion du risque appropriée peut entraîner une confiance irréaliste dans l'efficacité d'un système. Les conséquences pourraient inclure une erreur d'identification des individus recherchés, la fuite d'informations de listes de surveillance hautement sensibles ou l'insertion de code malveillant.

Les terroristes connus ou soupçonnés voyagent souvent sous des identités fausses ou falsifiées. Selon une perspective de gestion du risque, il s'avère donc important que ces systèmes traditionnels de correspondance biographique aient été correctement mis en œuvre (voir Section 3.1.4.). Les autorités nationales de gestion des frontières peuvent mettre en œuvre des recherches de vérification biométrique et de listes de surveillance afin de contribuer à atténuer le risque (voir Section 3.3.1.2).

La configuration d'un système biométrique dépend hautement du contexte. Par exemple, chaque aéroport est différent sur le plan de l'environnement et peut aussi varier en termes de démographie et de comportement des passagers. De là différents types de risques requérant des stratégies d'atténuation. Cependant, une stratégie d'atténuation du risque commune à tous porte sur l'exécution régulière de tests d'intrusion active par des testeurs experts afin de s'assurer de la mise à nu et de la compréhension des risques.

La gestion du risque est une activité spécialisée, gérée selon des normes internationales mais aussi leurs variantes nationales (voir les références à la fin de cette section).

La continuité de l'activité est un facteur crucial pour tout utilisateur et les protocoles d'urgence doivent former partie intégrante des procédures opérationnelles normalisées de tout système biométrique. Par conséquent, en cas de défaillance d'une quelconque partie d'un système et donc d'incapacité à assurer un service normal, il est habituel de disposer d'une ou plusieurs mesures exigeantes afin d'assumer une couverture de service temporaire. Il peut s'agir de l'intervention manuelle des opérateurs humains (ainsi des agents de la police des frontières assurant une tâche de vérification manuelle des passeports en cas de défaillance des portails biométriques automatiques) ou d'un retour à un système de sauvegarde ou une matrice de composants.[44]

2.3.1 Vulnérabilités et menaces émergentes

Aux fins de l'analyse, le panorama des menaces des applications biométriques de lutte contre le terrorisme a été ventilé selon les principaux domaines suivants :

- *Technologie de l'information générale :* Toute la technologie dorsale utilisée pour gérer les bases de données, sécuriser la transmission des informations, auditer l'activité des utilisateurs et éviter les virus. Elle devrait être couverte par les bonnes pratiques de sécurité IT pour les systèmes des organismes publics.
- *Environnement et capteurs biométriques :* Le type de technologie utilisée et les risques spécifiques. Ainsi l'usage de fausses empreintes digitales, de lunettes noires ou d'une technologie de modification de la voix.
- *Moteurs de correspondance biométrique :* La configuration des moteurs de correspondance incluant la configuration de seuil, la détection de présentation suspecte et la gestion des listes de surveillance.
- *Supervision humaine :* Tous les systèmes biométriques auront un certain niveau de taux de rejet et d'acceptation faux, particulièrement vrai dans le contexte des recherches de détection des crimes car les données biométriques enregistrées peuvent être de qualité variable (voir Section 1). Ces rejets et acceptations faux nécessitent examen et appréciation par des opérateurs dotés d'une formation appropriée. Une gestion incorrecte risque potentiellement d'entraîner l'arrestation des individus erronés, des pratiques professionnelles inefficaces, voire la perte de cibles de listes de surveillance présentant une menace élevée.

[44] Un bon exemple en est la Matrice redondante de disques indépendants (RAID - Redundant Array of Independent Drives) rencontrée communément dans les Système d'identification automatique d'empreintes digitales (AFIS). Cette configuration de lecteurs plus petits dans un serveur peut être combinée pour former une grande matrice qui améliore les performances et la sécurité tout en assurant également la redondance au sein du complexe de serveur. Pour la plupart, les utilisateurs des forces de l'ordre nécessitent que leur AFIS soit opérationnel 24/7/365. Par conséquent, l'arrêt du système pendant une période prolongée à des fins de maintenance, de mise à niveau ou de réparation n'est pas une option. L'usage souple de RAID dupliquées autorise donc le fonctionnement ininterrompu du système. En effet, même si plusieurs disques sont défaillants ou mis hors service, les données sont préservées sur les disques actifs pour assurer une prestation de service sans interruption pour l'utilisateur.

Table 1

Domaines de menace	Responsabilité	Conséquences	Exemples d'atténuation
Technologie de l'information générale	Responsables de la sécurité IT	Exposition de liste de surveillance, compromission de la sécurité du système, altération des correspondances. Modèle biométrique volé, employé pour la reconstruction de traits biométriques.	Sécurité des communications, logiciel antivirus, pare-feu (Déni de service), gestion des listes de surveillance biographiques, mise en interface sécurisée avec des systèmes externes. Données biométriques annulables.
Environnement et capteurs biométriques	Prestataire /Intégrateur de systèmes	Cibles de listes de surveillance capables d'éviter la détection en trompant un capteur	Configuration d'environnement, détection de présentation suspecte, filtrage de qualité. Algorithmes de lutte contre l'usurpation (détection d'attaque de présentation).
Moteurs de correspondance biométrique	Prestataire /Intégrateur de systèmes /Sécurité IT	Cibles de listes de surveillance capables d'éviter la détection	Réglage de système, gestion de la qualité d'enregistrement, gestion dorsale appropriée. Usage de données biométriques multimodales au lieu d'une modalité biométrique unique.
Supervision humaine	Organisme de sécurité du Gouvernement /Opérateurs	Arrestation des individus erronés, pratiques professionnelles inefficaces, perte de cibles de listes de surveillance présentant une menace élevée.	Instruction, formation et accréditation, audit, conception d'interface utilisateur, terminologie appropriée

2.3.2 Menaces par modalité

Les systèmes biométriques présentent un panorama de menaces complexe en évolution perpétuelle à mesure du déploiement toujours plus avant de la technologie. L'énoncé d'une répartition complète de tous les risques et vulnérabilités dans ce domaine échappe à la portée de ce document. Cependant, ils sont documentés dans la norme ISO/IEC 30107-2_2017 [1] mais aussi dans certains exemples spécifiques pour les organismes de gestion des frontières [2].

Les modalités biométriques communes utilisées à des fins de lutte contre le terrorisme sont les suivantes :

Visage - Le visage est communément disponible et facile à acquérir par des systèmes de capture à proximité ou à distance mais implique des contraintes techniques et des défis particuliers susceptibles de générer des images faciales de mauvaise qualité. Ces images affectent significativement la probabilité d'une détection correcte (ou inversement le nombre d'acceptations fausses générées par le système). La qualité de la photo d'enregistrement (celle employée afin de

créer la liste de surveillance) et celle de la photo d'une caméra peuvent avoir des répercussions. Le document de référence [3] offre des exemples d'amélioration de la reconnaissance faciale par surveillance. Les attributs qualitatifs spécifiques incluent : éclairage, pose, position de caméra, expression, couverture de tête, lunettes, barbes, résolution (pixels entre les yeux) et âge.
Certaines vulnérabilités communes du visage incluent :

- *Fraude par ressemblance :* Un document d'identité employé par une personne ressemblant au sujet prévu authentique. La personne sur une liste de surveillance peut ainsi prétendre ne pas être la cible correcte en cas de détection.
- *Masques :* Des masques en latex sophistiqués difficiles à détecter après une observation informelle deviennent disponibles.
- *Maquillage :* Pour éviter la détection, l'usage correct de maquillage peut masquer les caractéristiques faciales tout en demeurant naturel pour l'observateur humain.
- *Lunettes :* Les lunettes noires ou à monture épaisse peuvent masquer une part importante des caractéristiques faciales employées pour la reconnaissance.
- *Comportement :* Si des cibles soupçonnent qu'elles sont observées, l'usage d'un téléphone portable et le regard au sol peuvent rendre difficile la capture d'une image de qualité.
- *Morphose :* Des échantillons biométriques (ex. images faciales) de plusieurs donneurs fusionnés pour autoriser la vérification fructueuse de l'un quelconque des sujets donneurs par rapport à l'identité morphée.

Empreintes digitales - La biométrie des empreintes digitales est employée dans le monde entier par les forces de l'ordre. De nombreuses bases de données et listes de surveillance existantes contenant des modèles d'empreintes digitales coexistent donc (voir Section 1). Certaines vulnérabilités communes des systèmes biométriques à bases d'empreinte digitales incluent :

- *Faux doigts :* L'usage de fausses empreintes digitales composées de substances imitant les propriétés de la peau. Elles peuvent être portées individuellement sur chaque doigt ou intégrées dans un gant complet pour chaque main.
- *Dommage délibéré :* Si une cible soupçonne qu'elle risque d'être sous surveillance, elle peut tenter d'endommager ses empreintes digitales avec des produits chimiques, des substances abrasives ou d'autres techniques.
- *Empreintes digitales post mortem :* Des terroristes ont employé des impressions d'empreintes digitales de personnes décédées afin de créer des identités pour ouvrir des comptes bancaires et entreprendre des transactions financières afin de financer leurs opérations.

Iris - La reconnaissance de l'iris propose une modalité biométrique à la fois exacte et fiable. Elle est stable dans le temps et difficile à falsifier. Des travaux considérables de recherche et de développement sont en cours sur les systèmes de reconnaissance d'iris afin de lutter contre les usurpations mais aussi pour en faire une modalité alternative /additionnelle à des fins de gestion des frontières. Les vulnérabilités incluent :

- Usage de *lentilles de contact cosmétiques* présentant un motif d'iris imprimé.
- Usage d'images faciales de qualité supérieure disponibles sur Internet pour des *yeux imprimés*.
- *Dilatation des pupilles* dans toute la mesure du possible. De la sorte, le motif de l'iris ne peut pas être reconnu par un scanner (les performances de la reconnaissance d'iris se dégradent si un algorithme de correspondance est appliqué au même œil présentant une taille de pupille considérablement différente).

- *Lentille de contact à matrice de points* avec un faux motif directement sur l'œil de la personne. Elle peut empêcher le système de balayage d'iris de reconnaître un iris dans sa base de données.
- *Lentille sclérale avec iris peint dessus*. Ce type de lentille couvre l'intégralité de la zone visible du globe oculaire et la personne la portant présenterait l'apparence d'un motif oculaire complètement différent.
- *Implant chirurgical d'iris coloré* devant l'iris réel de la personne. Bien que nombre de personnes optant pour une chirurgie souhaitent uniquement modifier la couleur de leurs yeux, un individu désireux de masquer son identité pourrait aussi recourir à cette procédure.
- La correspondance exige des modèles de référence aisément disponibles durant l'authentification, créant pour un attaquant des opportunités de vol de ces modèles afin de faciliter ensuite de nouvelles attaques.

Voix - La technologie d'identification de locuteur peut être employée pour suivre les appels téléphoniques et déclencher des alertes sur des individus ciblés. Généralement, l'identification de locuteur présente une exactitude marginale pour de grands volumes de transactions ou de grandes bases de données (particulièrement sur différents canaux téléphoniques). Cependant, l'application de cette technologie peut s'avérer efficace si le nombre d'appels recherchés et le nombre d'individus sur la liste de surveillance sont relativement faibles et limités.
Certaines vulnérabilités communes pour la voix incluent :

- *Changeurs de voix :* Plusieurs applications sont disponibles pour les smartphones facilitant la modification de la voix.
- *Voix de synthèse :* Un vecteur de menace émergent relève de l'usage des outils qui peuvent être entraînés sur une voix de sorte à faire ensuite lire naturellement un message écrit par la voix de synthèse.

2.3.3 Qualité d'enregistrement

Indépendamment de la modalité, une biométrie de très mauvaise qualité peut ne pas mériter une inclusion dans une liste de surveillance. Si la qualité est insuffisante, la biométrie devrait probablement manquer des correspondances authentiques et risque de générer un nombre élevé d'acceptations fausses. La mesure et la gestion de la qualité biométrique sont des aspects importants de l'assurance d'un système biométrique exact. Chaque modalité dispose de ses propres mesures de qualité, ainsi le visage suscite des questions sur l'éclairage, la pose et les couvre-chefs. Tout facteur dégradant ou masquant l'élément biométrique durant le processus d'enregistrement affecte la capacité de recherche et de correspondance du système. La définition des mesures de qualité est couverte dans une suite de normes ISO (voir Section 2.4).

2.3.4 Rendement et gestion de capacité

Le rendement d'un système dépend naturellement des ressources informatiques disponibles pour l'établissement des correspondances et le traitement. La correspondance biométrique s'avère fréquemment un processus informatique coûteux, particulièrement pour les listes de surveillance longues. L'une des contraintes les plus importantes de la correspondance biométrique tient aux ressources humaines. Chaque correspondance à examiner exige l'appréciation d'un opérateur chevronné. En d'autres termes, par exemple, même en utilisant un système facial à l'équilibre de seuil

ajusté avec précision, le nombre de fausses acceptations à gérer dans un environnement affairé pourrait être considérable. La compréhension de ces exigences est une considération budgétaire importante, non seulement pour anticiper les impératifs de création initiaux mais aussi pour l'exploitation future.

2.3.5 Vol d'identité

En général, le vol d'identité correspond à l'acquisition sans autorisation des données à caractère personnel d'un individu, ainsi les noms, date de naissance, adresse et autres, afin de perpétrer des actes criminels, particulièrement la fraude comme l'usage de données volées pour effectuer de fausses demandes de prêts ou de cartes de crédit, voire pour acquérir des marchandises d'une valeur élevée. Le vol d'identité impliquant les données biométriques soulève des questions importantes car les caractéristiques biométriques demeurent habituellement avec une personne au long de toute sa vie et ne peuvent pas être facilement réinitialisées de la même manière qu'un mot de passe ou un code numérique d'identification personnelle. Le vol des données biométriques peut porter sur la biométrie physique elle-même de l'individu, ainsi la création d'une réplique d'empreintes digitales ou d'un masque facial, mais aussi sur le vol d'un modèle biométrique détenu dans une application ou une base de données. Plusieurs mesures d'atténuation majeures ont été développées pour combattre ces risques. Parmi les principales, nous relevons notamment :

Détection du caractère vivant : Divers capteurs sont intégrés dans des dispositifs de capture de biométrie pour voir au-delà du substrat de la biométrie présentée et différencier la peau vivante d'un artefact falsifié.

Données biométriques annulables : Lors de l'enregistrement des données biométriques dans un système, leurs caractéristiques sont intentionnellement déformées de manière répétables. Si le modèle est ensuite compromis ou volé, un modèle de remplacement des mêmes données biométriques est créé avec des caractéristiques de distorsion différentes de sorte que le modèle volé devienne immédiatement obsolète. Les mêmes données biométriques peuvent donc être utilisées dans une diversité d'applications mais les modèles sont tous différents. Les caractéristiques biométriques 'd'origine' - sans distorsion - ne sont jamais enregistrées, un synonyme de protection supérieure de la vie privée et d'apaisement pour l'utilisateur.

Il convient de noter que lorsque les données biométriques sont employées conjointement avec des documents d'identité (ainsi un passeport), le risque de vol d'identité est minimisé car si les données biométriques sont 'volées' ou copiées, l'attaquant nécessite tout de même un document valide qui peut être, si nécessaire, invalidé. Les données biométriques comme le visage peuvent être capturées de manière dissimulée ou via des sources en ligne par ceux désireux d'obtenir l'image. En d'autres termes, les autorités utilisant le visage comme donnée biométrique dans les documents formels devraient s'assurer d'avoir apprécié le risque de ce type de vol et adopté les mesures appropriées d'atténuation.

2.4 Normes internationales

2.4.1 Normes opératoires techniques

Il est essentiel que tout système biométrique de lutte contre le terrorisme soit sécurisé et constamment fiable tout en respectant les exigences d'activité spécifiques de l'utilisateur. Ces exigences reposent sur des facteurs clés comme :

- Tests de système pour s'assurer de la conformité avec les mesures et spécifications de performances présentes et futures
- Réseau et environnement d'exploitation sécurisés
- Appréciations des répercussions sur la vie privée et juridiques
- Gestion du risque pour un système de bout en bout
- Compétence d'opérateur démontrable
- Assurance d'intégrité et de gestion de données de toutes les caractéristiques de système, ainsi les dispositifs de capture de données biométriques, enregistrements de données et assurance des identifiants d'identité, stockage et extraction de données, performances de correspondance et taux d'erreur mais aussi toutes les métadonnées non biométriques
- Fiabilité logicielle et matérielle
- Interopérabilité - Transmission et échange de données avec d'autres systèmes
- Conception d'interface humaine – facilité d'utilisation pour (1) l'acquisition et l'enregistrement des personnes concernées et (2) opérateurs système - trousse à outils, poste de travail, ergonomie et environnement

Un vaste éventail de normes internationales, régionales et nationales couvre ces éléments essentiels et fonctions périphériques. Propriétaires, utilisateurs et clients des systèmes biométriques dépendent de ces normes pour assurer que leur application fonctionne efficacement sur l'ensemble de son cycle de vie et conformément aux spécifications de performances du fabricant. Ils dépendent aussi des normes pour disposer d'une assurance sur les processus comme les achats (voir Section 2.4), la maintenance et la mise à niveau du système biométrique, spécialement dans le cadre d'un réseau national ou international plus vaste qui échange des données. Il est improbable que des partenaires, potentiels ou non, d'un tel réseau acceptent de participer si certains membres du réseau n'exploitent pas leurs systèmes biométriques spécifiques en conformité avec les normes nationales ou internationales.

L'Organisation internationale de normalisation[45] (ISO) développe et publie des normes pour une ample palette de secteurs, notamment la biométrie et la criminalistique. L'ISO est une fédération mondiale d'organismes normatifs nationaux de 162 pays qui contribuent à la production de normes via leur appartenance à divers comités spécifiques par sujet. D'autres pays peuvent les rejoindre à titre de correspondant ou d'abonné pour recevoir des informations sur les normes.

L'ISO compte aussi deux comités conjoints avec la Commission électrotechnique internationale[46] (IEC - International Electrotechnical Commission) qui définit les normes et les Évaluations de la conformité (CA - Conformity Assessments) de tous les produits électriques, électroniques et connexes. Une évaluation de la conformité peut rassurer un acheteur potentiel, peut-être incapable de comprendre parfaitement les complexités du système ou du produit, sur son respect des normes techniques ou de sécurité requises, voire d'autres critères spécifiés. Nous relevons trois types de CA : *Première partie* La CA est menée par le fournisseur, *Seconde partie* La CA est menée par l'utilisateur mais la forme la plus rigoureuse de CA, *Tierce partie*, est menée par des organismes indépendants. Le processus est dénommé Certification car un certificat est habituellement délivré après une appréciation réussie. Son objet est de vérifier qu'un produit ou service respecte une certaine spécification ou norme ISO/IEC.

Les organismes régionaux peuvent aussi énoncer des normes afin d'harmoniser les systèmes et les pratiques professionnelles d'un groupe de pays. Ainsi, le Comité européen de normalisation[47] (CEN)

[45] http://www.iso.org
[46] http://www.iec.ch
[47] https://www.cen.eu

rassemble les organismes de normalisation nationaux de 34 pays européens et compte un Groupe de travail spécifique pour la biométrie (WG18) qui adapte les normes des organisations internationales ou nationales afin de respecter les exigences européennes comme la législation relative à la vie privée et à la protection des données.

Certaines normes sont définies à l'échelon national par l'organisation pertinente du pays, ainsi aux États-Unis, des organismes comme l'American National Standards Institute (ANSI) et le National Institute of Standards and Technology (NIST) définissent des normes appliquées à toutes les applications criminalistiques et biométriques associées. Les normes NIST ont été largement adoptées par nombre de pays dans des domaines clés comme la transmission électronique d'empreintes digitales en réseau. Le NIST conduit aussi des tests concurrentiels et assure un classement des algorithmes de comparaison et de recherche biométriques disponibles dans le commerce pour d'autres modalités biométriques comme le visage et l'iris.[48] Les acheteurs potentiels de systèmes de correspondance biométrique peuvent ainsi accéder à des informations objectives sur les performances relatives des algorithmes employés par des fabricants concurrents du marché international.

2.4.2 Normes opératoires scientifiques et procédures de gestion de la qualité

Outre les normes techniques et programmes de certification disponibles pour les systèmes biométriques, des normes ISO spécifiques s'appliquent aux procédures criminalistiques, ainsi la norme ISO/IEC 17025:2017 ' Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais'. Cette norme aborde les procédures et compétences nécessaires afin de mener des tests ou des étalonnages, notamment les échantillonnages. Elle examine la gestion des processus mais aussi la compétence et l'impartialité des scientifiques et la validité de leurs méthodes. Elle emploie des tests et des audits internes, menés par le laboratoire lui-même, et des audits externes et des tests de compétence, exécutés et supervisés par des organismes d'accréditation externes, afin de fomenter l'amélioration continue et d'accréditer le laboratoire. Ces inspections indépendantes régulières déterminent si le laboratoire respecte les normes requises pour obtenir ou préserver son accréditation selon la norme ISO17025:2017. Une Accréditation confirme que les laboratoires disposent d'un Système de management de la qualité (SMQ) parfaitement opérationnel en place et sont compétents pour exécuter des étalonnages et des tests scientifiques constamment en conformité avec la norme.

Le SMQ examine régulièrement tous les facteurs contribuant aux performances efficaces du laboratoire et, plus important, toute instance de défaut de conformité. Les procédures de mesures correctives servent à identifier la cause initiale d'un quelconque défaut de conformité alors que les actions de prévention sont formulées pour éviter toute récurrence. Les examens de gestion internes évaluent systématiquement les performances du laboratoire à l'aune d'une liste de contrôle complète d'exigences organisationnelles, de ressources, de processus et de gestion reposant sur le Manuel qualité du laboratoire.

Des normes peuvent être appliquées à d'autres domaines de la criminalistique comme les enquêtes criminelles (ainsi la norme ISO 17020:2012). Il s'avère donc possible et même très important d'adopter une approche normalisée des opérations de lutte contre le terrorisme couvrant l'ensemble des processus criminalistiques - de la scène de crime au tribunal - notamment :

[48] http://www.nist.gov

- Examen et gestion de scène de crime incluant les stratégies criminalistiques et biométriques (voir Section 3.3.3.2.) , appréciations interprétatives, coordination des ressources, méthodes d'échantillonnage, procédures anticontamination, matériels de conditionnement et examen des suspects, témoins et victimes.
- Processus de laboratoire incluant l'échantillonnage, les analyses, la gestion de base de données, la compétence du personnel et le reporting des résultats.
- Preuves judiciaires – Protocoles pour témoins experts, impartialité et techniques de présentation des preuves.

2.5 Achats et gestion des ressources

2.5.1 Achats

Les gouvernements nationaux comptent sur leurs propres critères de sélection et cadre réglementaire de travail pour maîtriser les achats de biens et services. Cependant, plusieurs points pertinents devraient être considérés à l'heure de l'appréciation du besoin d'un système biométrique et de certains aspects spécifiques connexes à l'achat des applications employées pour lutter contre la menace terroriste :

Exigences de l'activité – Les avantages et raisons du recours à la biométrie au lieu des formes alternatives de reconnaissance et d'authentification doivent être clairement articulés dans le plan d'affaires. Les avantages devraient être prudemment pondérés en regard des inconvénients potentiels comme le coût, les vulnérabilités techniques, les objections et résistances possibles du public et des clients, les préoccupations éthiques et les autres menaces identifiées par le processus d'Appréciation du risque. Les volumes d'utilisateurs et les niveaux de capacité des bases de données, présents et futurs, devraient être évalués prudemment pour assurer que le système pourra faire face aux rendements attendus, spécialement en cas de pic de fréquentation. (voir Section 2.3.4.).

Protection des données et de la vie privée – (voir Section 2.2) La capacité d'un système biométrique à identifier des terroristes connus ou soupçonnés doit se conformer aux droits des personnes au respect de leur vie privée et à la protection de leurs données à caractère personnel, conformément au droit national et international. Les systèmes biométriques peuvent commettre des erreurs soit par identification erronée, soit par défaut d'identification des personnes, chacun comportant des risques substantiels pour la réputation du ou des propriétaires des données. Ces aspects doivent être considérés posément durant la phase de conception de toute application biométrique et des procédures adéquates être mises en place pour gérer et atténuer ces occurrences si et quand elles surviennent.

NB Les ressources nécessaires pour étendre la mission d'un organisme de supervision de la vie privée existant ou pour la création d'un tel organisme (voir Section 2.2.7.) devraient être factorisées dans un plan de projet ou une politique régional ou national, cherchant à développer les systèmes biométriques de lutte contre le terrorisme.

Sécurité – Chaque composant d'un réseau ou d'un système biométrique exploitant des données liées aux terroristes et aux actes de terrorisme peut devenir la cible d'attaques physiques ou électroniques /cyber externes comme d'interférences ou de sabotages internes par la malveillance du personnel. Par conséquent, des niveaux élevés de sécurité par couches doivent protéger les environnements d'exploitation, matériels, logiciels, réseaux de communication et données stockées. Il conviendrait

aussi de considérer un processus de validation du personnel d'exploitation du système et de vérification de son niveau de vulnérabilité à une forme quelconque de coercition de la part des terroristes ou de leurs associés. Des audits réguliers devraient être menés afin d'identifier une corruption d'initié et des preuves de faute professionnelle. D'autres menaces comme les attaques de présentation (voir Section 2.3) doivent aussi être gérées et évitées dans le cadre d'une stratégie de sécurité globale.

Performances – Les applications biométriques au service de la lutte contre le terrorisme doivent être employées avec le degré le plus élevé d'exactitude. En d'autres termes, des taux d'erreur extrêmement bas sont impératifs tout en préservant un rendement acceptable. Nombre de vies peuvent être exposées au risque si le système n'arrive pas à identifier un terroriste, quelle que soit la raison, à un stade quelconque d'une opération. L'acquisition, la maintenance et la mise à niveau périodique de ce niveau de performances biométriques ne devrait pas nécessiter un financement significatif tout au long du cycle de vie du système. Ce risque élevé signifie aussi que les procédures de gestion des exceptions doivent être plus complètes et scrupuleuses pour éviter que les terroristes n'évitent délibérément les contrôles biométriques en faveur de systèmes de secours potentiellement moins rigoureux.

Modalité biométrique – La décision de sélection d'une ou plusieurs modalités particulières peut dépendre de facteurs comme :

- Accessibilité et fonctionnalité – Une décision d'achat fondamentale porte sur l'emploi, ou non, d'un mode biométrique unique pour l'application ou l'usage d'une approche multimodale. La ou les modalités sélectionnées doivent être adaptées aux tâches de comparaison de vérification (1:1) et d'identification (1:n) à entreprendre. Les systèmes monomodaux sont normalement moins coûteux à acquérir et exploiter mais ne peuvent pas faire face à chaque élément d'une population. Par exemple, il pourrait y avoir un nombre significatif de personnes impossibles à enregistrer dans un système d'empreintes digitales en raison de mains ou de doigts manquants ou endommagés de manière permanente ou de peau endommagée du fait d'exigences professionnelles, ainsi les individus travaillant avec des produits chimiques ou certains types de travaux manuels pouvant masquer, déformer ou détruire les crêtes papillaires de friction sur la surface des doigts et des mains. Si l'application biométrique doit enregistrer autant de personnes que possible, un système multimodal (ainsi des empreintes digitales et l'iris) est préférable car il peut capturer des données biométriques d'un pourcentage bien supérieur de la population concernée. Une décision d'achat similaire s'impose en termes de fonctionnalité. Ainsi, est-il conseillé d'acquérir une application biométrique gérant une fonction unique, comme un système d'empreinte digitales de fiches de police, ou l'investissement pourrait-il bénéficier d'une valeur ajoutée en créant un réseau multifonctionnel, comme des bases de données de casier judiciaire plus criminelles combinées simultanément avec des applications de gestion des frontières ? Il s'avère même possible d'étendre fonctions et modalités, si la législation nationale le permet, de sorte que le pays gère in fine un seul système biométrique. Certains pays commencent à adopter cette approche multimodale et multifonctionnelle afin d'assurer des économies d'échelle, de rationaliser les effectifs en personnel par la mise en commun de fonctions similaires pour qu'une seule structure de gestion et de gouvernance soit nécessaire pour un système national.
- Compatibilité des modalités et évolutivité – à l'heure de la sélection de la meilleure modalité pour une application de lutte contre le terrorisme, un aspect clé porte sur la probabilité de l'obtention et du partage de ces données avec des partenaires nationaux ou internationaux afin d'identifier les terroristes potentiels. Par exemple, un réseau régional de pays peut être

créé afin de partager des données d'empreintes digitales de tous les demandeurs de visa à l'entrée de leurs frontières respectives. Dès lors, tout pays souhaitant participer et bénéficier des avantages de ce réseau devrait utiliser des empreintes digitales pour ses systèmes biométriques de demande de visa même si une autre modalité était recommandée initialement, pour d'autres raisons, dans le cas d'étude d'origine. La prise en compte de certaines modalités en serait un prolongement car elles constituent aussi des données biométriques communes des scènes de crime et autoriseraient une recherche croisée à des fins de lutte contre le terrorisme. Par exemple, les empreintes digitales et le visage peuvent être préférés aux modalités d'iris et de veines des mains.

- Capture et enregistrement de données – ainsi, est-il préférable que le sujet soit en contact ou proche du dispositif de capture ou la capture à distance est-elle une meilleure option pour l'environnement d'exploitation ?
- Acceptabilité et opérabilité de rendement – certaines modalités biométriques peuvent être sujettes à des préjugés des clients, voire à une défiance sociale, ainsi les empreintes digitales sont souvent associées à la criminalité du fait de l'histoire policière. Certaines modalités peuvent être préférées car elles facilitent des procédures de capture et d'enregistrement plus rapides et aisées des données, souvent un facteur pour les applications nécessitant le traitement de volumes élevés de clients régulièrement (ainsi les point de contrôle aux frontières).

2.5.2 Gestion des ressources

L'achat d'une application biométrique majeure à grand volume exige un financement considérable en capital afin d'acquérir le matériel et le logiciel nécessaires et de créer des environnements d'exploitation adaptés et sécurisés, comme les postes de capture de données et d'enregistrement, salles de serveurs, suites d'opérateur, etc. En outre, pour certaines applications, des coûts peuvent être associés en termes de recrutement et de formation du personnel et, si une approche normalisée est employée, d'accréditation selon un roulement.

Une fois le système installé et les tests d'acceptation réussis, des travaux de maintenance réguliers sont à prévoir, de même que des mises à niveau de la sécurité et des performances logicielles occasionnelles à financer sur les budgets annuels. Ce financement vient s'ajouter aux charges salariales annuelles basiques de rémunération du personnel et de l'exploitation routinière efficace du système. Les systèmes biométriques doivent habituellement être opérationnels H24 chaque jour, tout au long de l'année et avec des arrêts minimisés.

La recherche et le développement modernes et commerciaux à l'échelon du globe dans les technologies biométriques introduisent constamment de nouvelles itérations logicielles et des capacités mises à niveau à un rythme élevé. Nombre de systèmes biométriques fonctionnent pendant vingt ans ou plus et nécessitent donc des actualisations répétées de leurs performances afin d'éviter toute obsolescence. Toute application biométrique peut être gravement compromise ou tout simplement défaillante en l'absence de mise à niveau et de maintenance régulières au fil de son cycle de vie[49].

[49] C'est pourquoi l'OACI impose l'usage des images au lieu des modèles dans les passeports électroniques. Cette évolutivité assure que les mises à niveau d'amélioration des algorithmes de correspondance demeurent une option pour leur intégration dans les systèmes d'inspection aux frontières reposant sur les données biométriques (habituellement des images faciales) lues sur les passeports électroniques.

Les procédures d'achat et de planification doivent aussi factoriser d'autres exigences futures, ainsi le besoin d'augmentation de la puissance de traitement pour faire face à la hausse de la demande, nécessitant dès lors un agrandissement de la capacité de stockage de base de données en résultante directe. Il peut aussi y avoir un besoin opérationnel de connexion et d'interopérabilité avec d'autres systèmes ou bases de données. L'un quelconque de ces progrès exigerait un financement futur additionnel, peut-être indisponible en cas de coupes budgétaires futures ou de priorité d'autres impératifs. Il est alors conseillé d'anticiper ces caractéristiques et exigences lors de la phase de planification et d'intégrer autant de ces facteurs que possible dans les nouveaux systèmes. Les applications devraient être pensées avec des capacités de réserve de traitement et de stockage ou compter sur des mises à niveau déjà budgétisées et convenues dans des contrats d'approvisionnement. La connectivité et l'interopérabilité avec d'autres systèmes pourrait aussi être intégrées dans un nouveau système si des capacités réseau sont envisagées initialement. Il s'avère considérablement moins coûteux de construire ces interfaces lors de la phase de conception plutôt que de les introduire ultérieurement ce qui risque d'affecter l'exploitation, voire d'exiger l'installation ou la reconfiguration des chemins et composants de connectivité dans les deux /tous les systèmes.

2.6 Pratiques recommandées

a) Les États devraient adopter une approche reposant sur les droits de l'homme de l'usage de la technologie lutte contre le terrorisme biométrique, incluant le recours à des mesures procédurales de protection et à une surveillance efficace de son application. Il s'agit là notamment de la création d'organes de contrôle appropriés et indépendants chargés de superviser la mise en œuvre de la législation pertinente relative à la vie privée et l'offre de recours efficaces en cas de violation, voire de l'élargissement du mandat des organes existants. Ces efforts pourraient être complétés par un processus d'examen éthique éclairant toutes les politiques et décisions nationales concernant l'utilisation de la biométrie à des fins de lutte contre le terrorisme.

b) L'application de la technologie biométrique afin de lutter contre le terrorisme international et la criminalité associée doit respecter les droits fondamentaux de tous les individus à la vie privée et à la protection légale de leurs données à caractère personnel, notamment les données biométriques.

c) Les systèmes biométriques peuvent être vulnérables aux défaillances et à maintes formes différentes d'attaque délibérée. Les États devraient donc procéder régulièrement à des appréciations du risque pour l'ensemble des processus de bout en bout de leurs applications biométriques afin d'atténuer les menaces existantes ou émergentes.

d) Il est recommandé aux États d'exploiter l'ensemble de leurs systèmes biométriques en conformité avec les normes techniques internationales et de rechercher une accréditation formelle de leurs processus criminalistiques et de gestion de la qualité, conformément avec les normes scientifiques internationales. C'est le gage non seulement de fondations solides pour un traitement biométrique efficace mais aussi une garantie pour des partenaires internationaux désireux de partager des données biométriques.

e) L'acquisition de systèmes biométriques exige une planification stratégique à long terme, abordant les exigences de ressources présentes et futures. Les États devraient donc considérer :

- Investissement initial en capital d'acquisition et de test du système
- Charges annuelles durables en personnel et maintenance de système plus mises à niveau de sécurité et de performances

- Budgets, capacité de base de données et puissance de traitement nécessaires pour le cycle de vie du système
- Connectivité et interopérabilité potentielles avec des réseaux nationaux ou internationaux et compatibilité des modalités
- Équilibre des exigences opérationnelles clés de tout système biométrique de lutte contre le terrorisme en termes de sécurité, d'accès et d'utilisabilité client, de volumes de fréquentation et de vitesse de traitement

2.6.1 Documents de référence

Résolutions du Conseil de sécurité des NU 1373(2001), 1624 (2005), 2178 (2014), 2195 (2014) et 2396 (2017) & Résolutions de l'Assemblée Générale des NU A/RES/68/276 et A/70/L.55

Publication de l'Agence des droits fondamentaux de l'Union Européenne 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights
http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975, par. 8; S/2015/939, Principe 15 (e).

Résolution du Conseil des droits de l'homme A/HRC/RES/34/7 (2017).

Commentaire général du Comité des droits de l'homme Nº 16 : Article 17 (Droit à la vie privée), par. 3-4.

Rapport du Rapporteur spécial sur le droit à la vie privée, A/HRC/31/64 (2016).

Déclaration universelle des droits de l'homme et PIDCP, préambule. PIDCP, Art. 2(1), 2(3), 9, 14 et 26.

Comité des droits de l'homme, commentaire général N° 16 (1988), voir :
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

Résolution AG 45/95 (1990) sur les principes directeurs pour la réglementation des fichiers personnels informatisés et Règlement général sur la protection des données de l'Union Européenne de 2018, Article 51 (Autorité de contrôle).

Rapport du Rapporteur spécial sur le droit à la vie privée, A/HRC/31/64 (2016).

Déclaration universelle des droits de l'homme, préambule.

Site Web du Fonds Monétaire International sur lequel les instruments de lutte contre le blanchiment d'argent et autres fraudes sont listés www.imf.org

Organisation internationale de normalisation http://www.iso.org

Commission électrotechnique internationale http://www.iec.ch

Comité européen de normalisation https://www.cen.eu

National Institute of Standards and Technology (États-Unis) http://www.nist.gov

Règlement général sur la protection des données de l'Union Européenne de 2018, Article 7 (Consentement), Article 17 (Droit d'effacement) et Article 15 (Droit d'accès aux données)

Article 19 du Pacte international relatif aux droits civils et politiques portant sur la liberté d'expression.

Document du HCR « Appréhender les questions de sécurité sans porter atteinte à la protection des réfugiés » http://www.refworld.org/docid/5672aed34.html

Déclaration des droits de l'homme des Nations Unies, Article 9 (Protection contre l'arrestation et l'exil arbitraires) et Article 10 (Droit à la présomption d'innocence)

Déclaration de Madrid des ministres des Affaires étrangères lors de la réunion spéciale du Comité contre le terrorisme du Conseil de sécurité du 28 juillet 2015.

Groupe Biometrics and Forensics Ethics du Royaume-Uni http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group

Principes directeurs en biométrie du Biometrics Institute pour un usage international www.biometricsinstitute.org

ISO/IEC 30107-2_2017: Détection d'attaque de présentation en biométrie. Formats des données

[2] Frontex, Vulnerability Assessment and Testing for Automated Border Control (Abc) Systems (2017)

[3] Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evaluation and Data Mining (2008) Springer.

ISO/IEC 27001:2013 Technologies de l'information -- Techniques de sécurité -- Systèmes de management de la sécurité de l'information -- Exigences

ISO 31000:2009 Management du risque -- Principes et lignes directrices

IEC 31010:2009 - Gestion des risques — Techniques d'évaluation des risques

NIST SP 800-30 Guide for Conducting Risk Assessments

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

ISO/IEC 17025:2017 Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais

3. Bases de données et systèmes biométriques de lutte contre le terrorisme

La section 3 propose un aperçu général des bases de données et systèmes biométriques de lutte contre le terrorisme actuels à l'échelle du spectre d'applications du maintien de l'ordre, de la gestion des frontières et militaires. Elle considère aussi les avantages du partage des données biométriques à un échelon bilatéral, multilatéral, régional et global et sur la manière dont les données biométriques, si elles sont employées avec d'autres données de renseignement, peuvent être exploitées de manière proactive afin d'empêcher des actes de terrorisme outre leur rôle traditionnel d'outil d'enquête. Les mesures prises par les autorités, en résultante de correspondances biométriques, sont alors appréciées à l'aune du droit international des droits de l'homme et de la nécessité d'une intervention légale et proportionnée en toute connaissance de cause. La partie finale de la section traite de l'inclusion de la biométrie dans les stratégies de lutte contre le terrorisme des États membres et des Régions et du rôle essentiel des organismes des forces de l'ordre et de contrôle des frontières dans le soutien actif de ces stratégies.

3.1. Bases de données et systèmes biométriques de lutte contre le terrorisme actuels

3.1.1. Applications de gestion des frontières

Sans cesse plus sophistiquée, la gestion des frontières[50] joue un rôle crucial dans la lutte contre le terrorisme au sens large et dans l'interception des combattants terroristes étrangers en particulier. Dans une large mesure, la modalité de transport détermine les caractéristiques et la portée des points de franchissement des frontières (PFF). Pour les voyages aériens internationaux, les PFF sont hautement normalisés. Pour les voyages par voie terrestre ou maritime, nous relevons typiquement deux types de PFF : l'un pour les voyageurs internationaux et l'autre réservé à l'usage des nationaux transfrontaliers. Les voyageurs internationaux ont une obligation de déclaration au PFF pour entrer légalement dans un pays. Les PFF des populations locales sont, en général, situés au niveau des frontières terrestres ou de ports désignés desservant plusieurs États proches. Ces PFF locaux sont souvent mis en œuvre conjointement avec des zones économiques où la ligne de démarcation se situe en général à 25 km à l'intérieur des terres de chaque côté et est ouverte aux nationaux de chaque côté de la frontière. Ces PFF locaux ne peuvent pas être employés par d'autres voyageurs internationaux.

Les PFF aux frontières internationales agissent comme des filtres efficaces pouvant être étendus ou contractés selon le niveau des menaces. En général, le filtre est un niveau 'Normal' mais, lorsque les menaces s'accroissent, il passe en Code Orange ou même en Code Rouge (ou des alertes équivalentes) et, dans des situations extrêmes, la frontière se ferme complètement. Dans des situations où un grand nombre de personnes peuvent devoir entrer rapidement dans le pays, ainsi en cas de désastre naturel

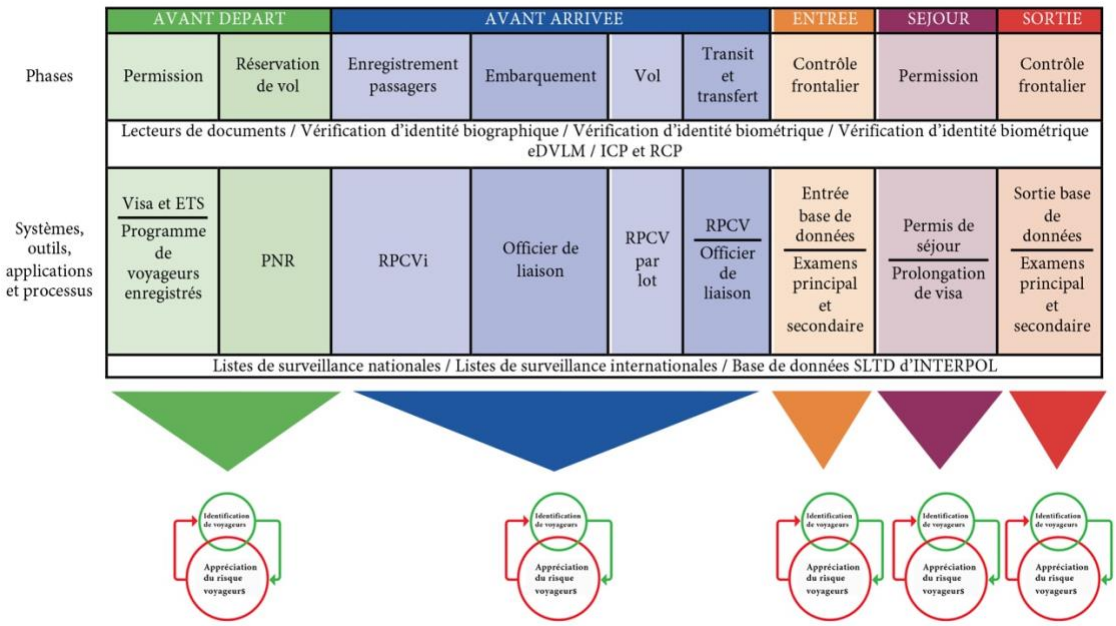
[50] « La 'Limite territoriale' est habituellement utilisée en référence à la ligne séparant le territoire ou l'espace maritime de deux États alors que la 'Frontière' est une ligne à franchir pour entrer dans un État. Parfois, elles coïncident exactement mais il est plus fréquent que les frontières incluent des infrastructures comme les points de contrôle d'immigration, les installations douanières, les barrières et les routes de patrouille allant au-delà de la limite territoriale. Dans le cas des aéroports et ports maritimes internationaux, la frontière peut se trouver à des centaines de kilomètres de la limite territoriale. Une limite territoriale est essentiellement une ligne de définition alors que la frontière constitue habituellement une entité plus complexe comprenant plusieurs lignes ou zones et dont la fonction primaire est la régulation des mouvements de personnes et de marchandises. » *Professeur Martin Pratt de l'Université de Durham au Royaume-Uni*

ou artificiel dans un pays voisin, la frontière peut être ouverte afin de faciliter l'accès alors que les contrôles formels nécessaires sont effectués ultérieurement dès que les personnes ont atteint des zones de sécurité au-delà de la frontière.

Le contrôle frontalier des voyageurs et marchandises est confié aux organismes responsables de l'immigration, du contrôle d'accès et de la sécurité, du maintien de l'ordre, des douanes et de la quarantaine. Les organismes de gestion des frontières nécessitent un environnement de travail efficient, un personnel motivé et bien formé, une technologie sophistiquée et des informations actualisées. L'ajout d'applications biométriques est un élément important des PFF modernes, facilitant grandement les processus de gestion des frontières. Elles forment partie d'une approche technologique plus vaste qui couvre tous les aspects des déplacements transfrontaliers du point initial d'organisation du voyage jusqu'au point d'arrivée et au départ final du visiteur. Les informations recueillies à chaque phase de ce processus sont compilées de différentes sources et communiquées au responsable de la gestion des frontières qui les emploie, avec d'autres données, afin de décider de l'autorisation, ou non, d'entrée du voyageur dans le pays.

Le domaine du voyage aérien international est le plus développé et a suscité, par le passé, l'innovation technologique reposant sur des normes qui a ensuite été appliquée aux frontières terrestres et maritimes. Ce profil durable devrait perdurer dans le cadre de l'usage émergent de la biométrie afin d'identifier les terroristes. L'architecture moderne de contrôle frontalier pour le voyage aérien international facilite la répétition de l'identification des voyageurs et de l'appréciation du risque au fil du déplacement du voyageur à mesure que des informations additionnelles deviennent disponibles à l'État de destination ou de départ. Les principales sources de données sur les voyageurs pour le domaine du voyage aérien international sont les compagnies aériennes et les gouvernements, les solutions émergentes pour l'application de la biométrie préservant ces deux mêmes sources de données.

Figure 4 – Les cinq phases du continuum du déplacement[51]
(Avec la permission de l'OACI)



Selon la perspective des états de destination, le processus de bout en bout se divise en cinq phases (voir Fig. 4) :

1. Avant le départ
2. Avant l'arrivée
3. Entrée
4. Séjour
5. Sortie

Selon une perspective internationale à l'échelle de tout le système, le déplacement constitue un continuum car le processus de sortie de l'État où le déplacement commence correspond au processus avant l'arrivée des États de transit et de destination pour ce déplacement.

Phase 1 : Avant le départ

Aujourd'hui, nombre d'États exigent des informations préalables de tous les voyageurs avant leur arrivée à la frontière. Ces informations correspondent principalement à des détails biographiques, de la documentation et des données sur le déplacement. De plus en plus, les États exigent aussi des informations biométriques afin de pouvoir confirmer l'identité des nationaux étrangers qui arrivent. Par le passé, ces voyageurs pouvaient être divisés en deux groupes, à savoir ceux nécessitant un visa d'entrée sur le territoire et ceux en étant dispensés. Depuis les années 1990, les données du système de contrôle des départs des compagnies aériennes sont accessibles aux États sous la forme des renseignements préalables concernant les voyageurs (RPCV) et des RCPV interactifs. Aujourd'hui, les

[51] Voir l'ICAO TRIP Guide on Border Control Management, Montréal (2018) pour en savoir plus.

États recueillent les informations des voyageurs avant leur déplacement via un éventail de mécanismes. Les systèmes et processus suivants sont actuellement employés pour la collecte des informations nécessaires préalables à l'arrivée :

1.a. Demande de visa 'classique' **-** Une exigence commune dans nombre de pays qui repose sur des facteurs historiques, diplomatiques et économiques mais aussi sur les relations politiques des états. Le processus implique habituellement la soumission par le demandeur d'attributs identitaires biographiques et biométriques via un processus de demande exhaustif qui inclut l'envoi de documents de voyage et une redevance pour le représentant ou le poste diplomatique du pays de destination. Les données biométriques peuvent être une photo du visage ou un enregistrement comme un jeu d'empreintes digitales. La demande est alors évaluée et un visa est ensuite délivré ou refusé. L'évaluation avant la délivrance peut inclure une recherche 1:n sur une liste de surveillance biométrique pour les états disposant d'ensembles de données compilés à cette fin.

1.b. Demande de visa régional **-** La collaboration régionale entre pays est commune et chaque continent compte au moins une entité régionale, ainsi l'ASEAN[52] en Asie du Sud-Est, la CEDEAO[53] en Afrique occidentale, l'UE en Europe, l'UNASUR[54] en Amérique du Sud et la CARICOM[55] dans les Caraïbes. Le niveau de coopération entre ces entités diffère. L'Union Européenne est un exemple d'un tel système régional. Elle a adopté une réglementation qui exige de chaque État membre la mise en œuvre de son propre Système européen d'identification des visas (SIV). Ces systèmes sont connectés avec la plateforme SIV centrale qui est gérée par l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA). Le SIV utilise des contrôles biométriques sous forme de photo du visage et de jeu de dix empreintes digitales pour vérifier l'identité des voyageurs à la frontière plus un contrôle biographique via le Système d'information Schengen II (SIS-II)[56] et des bases de données nationales. L'architecture de ces systèmes régionaux facilite l'intégration de l'évaluation avant la délivrance qui peut inclure une recherche 1:n sur une liste de surveillance biométrique pour les États et régions disposant d'ensembles de données compilés à cette fin.

1.c. Application externalisée Ce modèle, toujours plus populaire dans nombre d'États, emploie des prestataires commerciaux pour la collecte et la compilation de toute la documentation et des informations du demandeur, nécessaires pour le processus de demande de visa. Le processus d'activité peut aussi enregistrer des données biométriques du demandeur (images faciales, scans d'iris ou empreintes digitales). La demande complète est transmise au poste diplomatique approprié afin de mener les contrôles nécessaires et de décider de la délivrance, ou non, du visa. L'évaluation avant la délivrance peut inclure le renvoi d'une image ou d'un modèle biométrique à l'État pour une recherche 1:n sur une liste de surveillance biométrique pour les États disposant d'ensembles de données compilés à cette fin.

---

[52] ASEAN Association of South East Asian Nations (Association des nations de l'Asie du Sud-Est)

[53] CEDEAO Communauté économique des États de l'Afrique de l'Ouest

[54] UNASUR Unión de Naciones Suramericanas (Union des nations sud-américaines)

[55] CARICOM Caribbean Community (Communauté des Caraïbes)

[56] L'eu-SIS-II fomente la sécurité publique, le contrôle des frontières et la coopération des forces de l'ordre en Europe entre les États signataires du Traité de Schengen. Les informations des bases de données de la police et des listes de surveillance de la gestion des frontières sont partagées entre les États. Ces informations sont accessibles dans les pays et aux frontières mais aussi employées pour contrôler les personnes entrant et sortant de l'Union Européenne. Le système contient les données des personnes recherchées et disparues, des documents d'identité /voyage perdus ou volés, de biométrie, des véhicules volés, etc.

1.d. Demande de visa électronique /en ligne Le processus de demande est conduit entièrement en ligne via des formulaires électroniques et des images numérisées de la photographie du demandeur (conformité OACI) et de la page biographique du passeport. Le processus de prise de décision et toute évaluation biométrique sont centralisés. Si le visa est délivré, le demandeur reçoit la confirmation et un contrôle de vérification 1:1 biométrique intervient à la frontière par comparaison du visage du demandeur avec la photo soumise afin de confirmer que le demandeur et le voyageur sont bien la même personne. L'évaluation avant la délivrance peut inclure une recherche 1:n sur une liste de surveillance biométrique pour les États disposant d'ensembles de données compilés à cette fin.

1.e. Systèmes électroniques de voyage (ETS) Ce processus recueille des données d'identité de base des voyageurs indépendamment des exigences de visa. Il est similaire par son fonctionnement au visa électronique /en ligne mais des données biométriques autre qu'une photo du visage sont obtenues à la frontière et non lors de la phase avant le départ.

L'autre source majeure de données sur les voyageurs avant le début du déplacement est constituée par les compagnies aériennes :[57]

1.f. Le système des Données des dossiers passagers (PNR) Après l'obtention par le voyageur d'un visa /autorisation de voyage, la phase suivante passe par la réservation d'un vol en renseignant le formulaire PNR en ligne. Les données PNR sont stockées dans le Système de réservation informatique (CRS - Computer Reservation System) de la compagnie aérienne pour son propre usage commercial et opérationnel mais est aussi disponibles pour les organismes de gestion des frontières avant le départ du voyageur. L'OMD, l'IATA et l'OACI ont créé et gèrent des normes techniques (PNRGOV)[58] pour l'échange harmonisé de données PNR entre les exploitants de compagnie aérienne et les gouvernements. *Aucune donnée biométrique n'est contenue dans un enregistrement PNR.* La valeur des données PNR tient à ce qu'elles offrent d'importantes informations contextuelles pour améliorer l'assurance de l'identité et pour informer sur le ciblage selon le risque des voyageurs d'intérêt.

Phase 2 : Avant l'arrivée

2.a. Les *Renseignements préalables concernant les voyageurs (RPCV* sont créés dans les systèmes de contrôle des départs des compagnies aériennes. Les RPCV sont compilés progressivement à l'enregistrement des passagers mais uniquement envoyés aux organismes publics de destination une fois que les voyageurs sont enregistrés, qu'ils ont embarqué dans l'aéronef et que les portes de l'aéronef ont été fermées. Notablement, les RPCV sont complétés lors des arrêts de transit pour les longs courriers. Les RPCV emploient deux sources de données : (1) les informations de la Zone de lecture automatique (ZLA) du passeport des voyageurs et (2) les détails des informations de vol et d'enregistrement des passagers, pouvant inclure des éléments de données aussi bien normalisés qu'additionnels comme les bagages enregistrés, les numéros de siège, le nombre de passagers en vol ainsi que le numéro, la date, l'heure et les lieux de départ et d'arrivée du vol. L'organisme destinataire peut ainsi exécuter un contrôle préalable de tous les passagers avant leur arrivée. La norme aujourd'hui établie pour la transmission des données RPCV *n'a pas inclus les données biométriques bien qu'il soit possible à l'avenir de collecter une photo conforme OACI sur la puce sans contact du passeport /document de voyage. L'installation d'un lecteur de passeport électronique sur les terminaux*

[57] Pour les PNR et RPCV, l'Annexe 9, 15e édition, de la Convention de Chicago, recueille des normes et pratiques recommandées en son chapitre 9 « Systèmes d'échange de données sur les passagers ». Le message électronique standard, incluant des ensembles de données, a été développé et convenu conjointement entre les organismes OMD/IATA/OACI dans les Lignes directrices sur les données des dossiers passagers (Doc 9944) et les RPCV.

PNRGOV EDIFACT & XML Message Implementation Guide: www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

ou comptoirs d'enregistrement des passagers serait alors nécessaire et les pays ne disposent pas actuellement tous de cette technologie.

2.b. Renseignements préalables concernant les voyageurs interactifs (RPCVi) Il s'agit là d'une version améliorée des RPCV car les informations des voyageurs sont transmises à l'organisme destinataire désigné dès l'enregistrement électronique des passagers. Elles sont envoyées individuellement et non par lot comme pour le processus RPCV. Grâce au processus RPCVi, les contrôles de liste de surveillance et autres sont exécutés avant que le voyageur n'embarque dans l'aéronef ce qui offre un surcroît de protection pour la compagnie aérienne, pour ses passagers et pour le pays de destination. *Les éléments biométriques seraient similaires à ceux des RPCV précédemment mentionnés en 2a.*

Étude de cas 5 – Entrée sans présentation de document de voyage

Un plan d'usage de portails de Contrôle des frontières automatisé (CFA) pour les déplacements entre l'Australie et la Nouvelle Zélande est aujourd'hui à l'étude. Il exploiterait les systèmes RPCVi existants et associerait les images faciales disponibles sur les passeports et les bases de données de visa afin de générer une base de données dynamique des arrivées prévues pour chaque voyageur arrivant par avion. Pour cette application, le passeport électronique demeure dans la poche du voyageur et les portails biométriques CFA comparent l'image faciale du voyageur avec celle de la base de données des arrivées prévues, autorisant l'entrée uniquement si les deux correspondent. La solution développée est une application à faible échelle de l'identification biométrique 1:n.

Nombre d'États complètent leur filtrage préalable à l'arrivée par le déploiement d'officiers de liaison, des responsables publics des états de destination, travaillant auprès des compagnies aériennes dans les aéroports d'embarquement et de transit pour faciliter l'identification des voyageurs et l'appréciation du risque.

Phase 3 : Entrée

Un passager peut uniquement voyager si tous les protocoles préalables à l'arrivée sont réussis. Cependant, pour la plupart des juridictions, l'exécution des processus de la Phase 1 Avant le départ et la Phase 2 Avant l'arrivée ne garantit pas l'entrée dans le pays à l'arrivée. Une décision définitive est prise par le responsable du contrôle à la frontière lorsque le voyageur présente les documents et identifiants nécessaires à son arrivée. Le responsable de l'immigration doit fonder sa décision sur divers facteurs. Des Systèmes d'information de gestion des frontières (BMS - Border Management Information Systems) ont donc été développés pour faciliter ce processus. Il convient toutefois de noter que certains PFF ne disposent pas encore d'un accès à la technologie BMS. Les BMS varient grandement par la sophistication de leurs fonctionnalités. Dans les juridictions les plus sophistiquées, la vérification de l'identité biométrique ne cesse de croître. L'application des listes de surveillance biométriques est bien moins commune. Les principales variantes sont les suivantes :

3.a Système d'information de gestion des frontières (BMS) standard La législation et le droit nationaux contrôlent le nombre et le type de vérifications menées à la frontière, soit l'enregistrement, ou non, des détails de tous les voyageurs qui entrent dans un pays ou la simple exécution de recherches sur des listes de surveillance ou de sanctions. Les pays qui enregistrent toutes les arrivées de voyageurs nécessitent un BMS sous une forme ou une autre. Les données peuvent être enregistrées manuellement mais, pour la plupart, les systèmes modernes emploient un lecteur de passeport pour charger les données de la Zone de lecture automatique du document de voyage et le responsable du contrôle à la frontière saisit des informations additionnelles concernant l'identité, la durée et le motif de la visite, l'adresse dans le pays, etc. Les données sont alors recherchées dans les listes de

surveillance. *Un BMS standard ne capture pas les données biométriques à des fins de vérification automatisée.*

3.b. Système électronique d'information de gestion des frontières (e-BMS) Un e-BMS emploie un lecteur de passeport électronique pour accéder à la puce sans contact embarquée dans le Document électronique de voyage lisible à la machine (eDVLM)[59]. Cette puce contient les données ZLA ainsi que la photo numérique conforme OACI du visage et souvent également deux empreintes digitales. Dans certains pays, ces empreintes digitales sont uniquement accessibles à des fins de vérification si l'e-BMS contient un certificat numérique du pays de délivrance autorisant l'ouverture du groupe de données renfermant les empreintes digitales. Afin de vérifier les identités des données biométriques embarquées dans la puce, un e-BMS doit être connecté à un système biométrique et pouvoir capturer les données biométriques du voyageur avec une caméra pour le visage, une caméra infrarouge pour l'iris ou un scanner pour les empreintes digitales à des fins de comparaison avec les données de la puce. Un eBMS est compatible avec les contrôles 1:1 de vérification d'identité biométrique exploitant les images des caractéristiques biométriques lues sur le passeport électronique. Un eBMS peut inclure une recherche 1:n sur une liste de surveillance biométrique pour les États disposant d'ensembles de données compilés à cette fin.

Les terroristes peuvent utiliser des documents de voyage frauduleux pour franchir les frontières sans être détectés. Les tactiques employées vont de l'usage d'une photographie de substitution au recours au passeport d'une personne semblable d'apparence, voire la création d'un faux d'un document complet. Un lecteur de passeport électronique autonome, lié à un système biométrique intégré, s'avère donc un outil précieux d'examen de document pour lutter contre la fraude au passeport, spécialement sur les PFF disposant de ressources limitées pour contrecarrer ce genre de fraude. L'installation de cet équipement dans un site secondaire peut grandement faciliter les enquêtes des responsables du contrôle à la frontière pour les voyageurs dont les documents ont suscité des soupçons au PFF.

Étude de cas 6 – Structure de données logique Version 2

La Structure de données logique (SDL) Version 2 est un nouveau développement susceptible de faciliter l'accès à d'autres données biométriques enregistrées dans les passeports électroniques. La SDL est stockée dans la puce sans contact du passeport électronique ou du document de voyage et peut être comparée avec une 'armoire' contenant 16 tiroirs dénommés Groupes de données. Certaines des informations stockées sont obligatoires mais l'inclusion d'autres éléments est optionnelle, à la discrétion de chaque pays. Les Groupes de données doivent être en conformité avec la structure OACI – ICP[60]. C'est le gage que les données contenues dans la SDL ont été délivrées par une autorité authentique sans altération, ni révocation. La SDL-2 ajoute trois nouveaux éléments à la structure SDL, à savoir (1) les tampons d'entrée et de sortie des dossiers de voyage, (2) les dossiers de visa et (3) des données biométriques additionnelles. La SDL-2 peut être stockée sur la puce sans contact du passeport électronique à la discrétion de l'autorité de délivrance à l'occasion de la délivrance des passeports électroniques.

[59] eDVLM - Un DVLM (passeport ou carte) embarque un circuit intégré sans contact et dispose de la capacité d'être employé pour l'identification biométrique du titulaire du DVLM selon les normes spécifiées dans la partie concernée du Document OACI 9303 — Documents de voyage lisibles à la machine

[60] L'ICP (Infrastructure à clés publiques) est définie par l'OACI comme un ensemble de politiques, de processus et de technologies servant à vérifier, enregistrer et certifier des utilisateurs d'une application de sécurité. Une ICP emploie des pratiques de cryptographie à clé et de certification à clé pour sécuriser les communications.

En d'autres termes, les autorités de contrôle des visas et des frontières peuvent désormais rédiger des informations, relevant des trois nouveaux Groupes de données, dans la puce sans contact d'un autre pays. Les dossiers de voyage peuvent alors être stockés par l'organisme de contrôle des frontières, en validant le passeport électroniquement, et les détails de visa peuvent être à nouveau saisis dans le Groupe de données par les autorités concernées, avec une possible vérification électronique à l'arrivée à la frontière. Les voyageurs enregistrés dans les programmes de voyage déclarés pourraient voir leurs modèles biométriques pertinents stockés dans leur passeport électronique à des fins d'usage dans les portails CFA des pays participants.

NB La rédaction de nouvelles données dans la puce sans contact est soumise à la condition juridique d'un échange de certificats OACI-ICP entre l'autorité de délivrance du passeport électronique et le pays souhaitant ajouter les données. La SDL-2 ne peut pas être employée si cette condition juridique n'est pas respectée.

3.c. Système électronique d'information de gestion des frontières et des données biométriques (e-2BMS) Il est similaire à l'e-BMIS mais sans utiliser de lecteur de passeport électronique car les données biométriques sont enregistrées à la frontière et via le système de visa. Ce système offre l'avantage que l'intégralité du processus biométrique est détenu par le pays de destination. Les responsables publics peuvent ainsi maîtriser la qualité des enregistrements pour maximiser les performances du système de correspondance 1:1 de vérification biométrique. Par exemple, grâce à l'adoption de cette architecture par les États-Unis, les contrôles de listes de surveillance biométriques 1:n peuvent être intégrés avec les dossiers de listes de surveillance exhaustifs compilés par le Gouvernement des États-Unis de tous les titulaires de passeport étrangers à leur arrivée.

3.d. Système de contrôle des frontières automatisé (CFA) - La croissance exponentielle du nombre de passagers internationaux ces dernières décennies a stimulé l'innovation technologique et l'automatisation aux frontières. Depuis le premier système de contrôle des frontières automatisé à l'aéroport de Schiphol aux Pays-Bas, les systèmes CFA se sont disséminés dans le monde entier pour devenir aujourd'hui d'un usage régulier dans nombre de pays. Les itérations modernes du système emploient des capteurs haute vitesse et des données biométriques stockées dans la puce des documents de voyage électroniques, ainsi le visage, l'iris et les empreintes digitales pour compléter la vérification 1:1 des données biométriques et faciliter l'entrée automatique par les portails frontaliers. De là le passage rapide de groupes prioritaires ou de nationalités pré-qualifiées via les PFF à haute fréquentation dans un délai minimum et la libération des responsables du contrôle de la frontière pour se concentrer sur d'autres voyageurs pouvant nécessiter une inspection plus attentive. Les autorités nationales ou régionales décident des nationalités ou groupes pouvant utiliser les portails CFA à un moment donné, selon les appréciations du risque actuel et la législation connexe. Les solutions CFA peuvent inclure une recherche 1:n sur une liste de surveillance biométrique pour les États disposant d'ensembles de données compilés à cette fin.

Phase 4 : Séjour

Chaque pays est responsable de la gestion des non-nationaux pouvant visiter brièvement, séjourner plus longuement ou résider à l'intérieur de ses frontières. Cette tâche peut incomber à différents organismes et autorités, selon les législations et réglementations nationales mais les rôles demeurent similaires, soit la délivrance de permis de résidence et d'études, le traitement des demandes d'asile et de réfugiés et les demandes de naturalisation ainsi que les devoirs de maintien de l'ordre comme le traitement des délits liés au séjour illégal, à la traite des êtres humains, à l'exploitation de la main-d'œuvre, etc.

Au niveau régional, les systèmes eu-VIS et eu-SIS-II de l'Union Européenne, décrits lors de la Phase 1.b. plus haut, en sont de bons exemples. Grâce à ces bases de données, les autorités concernées des pays de l'UE peuvent gérer les nationaux étrangers dans le cadre de leurs frontières respectives. En outre, nous relevons aussi Eurodac qui est une base de données centralisée de l'UE qui collecte et traite les empreintes digitales numérisées des demandeurs d'asile. Elle est actuellement employée par 28 pays de l'UE mais aussi par la Norvège, l'Islande, la Suisse et le Liechtenstein. Eurodac traite, stocke ou compare les empreintes digitales des apatrides ou des nationaux des pays tiers ayant 14 ans révolus et (1) ayant demandé l'asile dans l'un quelconque des pays participant à Eurodac, (2) ayant été appréhendés en connexion avec le franchissement irrégulier d'une frontière externe ou (3) dont la présence dans un pays Eurodac a été estimée illégale. Eurodac joue aussi un rôle important dans l'exécution du Règlement de Dublin. Il régit les demandes des demandeurs d'asile et est censé éviter les demandes d'asile multiples dans différents pays de l'UE. Ce règlement a pour principal objet d'assigner une responsabilité de traitement des demandes d'asile à un État membre unique, le plus souvent le pays de première entrée dans l'UE du demandeur d'asile pour son traitement ultérieur. Depuis juillet 2015, les autorités de maintien de l'ordre disposent d'un accès limité à Eurodac, sous des conditions très strictes, pour conduire des recherches d'empreintes digitales ciblées. Elles doivent être menées au cas par cas et uniquement en connexion avec la prévention, la détection et l'enquête de certains crimes graves et délits de terrorisme.

Les données biométriques collectées par les organismes de contrôle des frontières durant les premières phases du voyage peuvent, dans un contexte approprié d'enquête ou de collecte de renseignements, être partagées par les organismes de sécurité et de maintien de l'ordre.

Phase 5 : Sortie

Le processus préalable au départ est similaire aux protocoles préalables à l'arrivée. Le voyageur doit effectuer son enregistrement passager en ligne ou à l'aéroport et présenter ses documents avant d'embarquer dans l'avion. Les systèmes CFA sont complétés par un nombre de programmes de voyageurs fréquents comme le « Programme des voyageurs enregistrés ». Ces programmes exigent d'un voyageur son adhésion, l'enregistrement de données biométriques et parfois un processus d'évaluation. Les États-Unis, par exemple, comptent sur le programme Global Entry qui assure un contrôle accéléré pour les voyageurs à faible risque préalablement approuvés lorsqu'ils passent les frontières des États-Unis. Les membres du programme passent par les kiosques Global Entry spécifiques, présentent leur passeport lisible à la machine ou le carte de résident permanent des États-Unis, posent leurs doigts sur le scanner pour une vérification des empreintes digitales et renseignent une déclaration douanière. Le kiosque délivre au voyageur un reçu de transaction. Le programme Global Entry nécessite une approbation préalable des voyageurs. Tous les demandeurs doivent subir une enquête sur leurs antécédents et un entretien en personne avant leur enregistrement.

Bien que les pays ne conduisent pas tous un contrôle de sortie d'immigration à l'heure du départ, nombre d'entre eux contrôlent tout de même un voyageur avant son départ du pays. Il implique habituellement une vérification que le nom indiqué sur la carte d'embarquement correspond à celui mentionné sur le document de voyage et à sa recherche dans les listes de surveillance biographiques, que les détails du vol sont cohérents avec les horaires des vols du jour et que le voyageur n'a pas dépassé les dates de son autorisation de séjour. Outre ces contrôles, ils assurent aussi une appréciation des voyageurs, recherchant les passeurs de drogues et d'argent, les trafiquants dans d'autres pays et spécialement les combattants terroristes étrangers, sur la base du document de voyage, de la carte d'embarquement et d'autres critères spécifiques.

Étude de cas 7 – Vérification biométrique au départ

Aux États-Unis, un modèle de partenariat émerge pour les compagnies aériennes, les aéroports et le Gouvernement afin d'investir dans des initiatives de facilitation aux portails d'embarquement, assurant un mécanisme alternatif pour l'obtention d'une vérification biométrique au départ. Début 2018, Lufthansa et British Airways ont entrepris des tests de reconnaissance faciale. Il s'agit là d'une nouvelle application de la vérification biométrique *1:n* des voyageurs connus, analogue aux ententes en cours de développement dans les partenariats compagnie aérienne-Gouvernement pour les déplacements entre l'Australie et la Nouvelle Zélande (voir Étude de cas 5).

3.1.2 Applications policières et INTERPOL

Les bases de données biométriques employées pour le maintien de l'ordre sont habituellement composées de Données de référence des prévenus (images faciales, empreintes digitales et profils ADN), de données de scène de crime et d'autres données non identifiées, ainsi des enquêtes sur des personnes disparues ou décédées ou des activités de collecte de renseignement. Ces systèmes peuvent être exploités à l'échelon local, provincial ou national pour remplir des fonctions comme la gestion des casiers judiciaires, les enquêtes criminelles ou la génération de produits de renseignement criminalistique. Les données biométriques générées par les enquêtes sur le terrorisme peuvent être soit ajoutées à ces systèmes, soit chargées dans des bases de données dédiées présentant des mesures de sécurité additionnelles. Indépendamment de la configuration de base de données employée, un besoin opérationnel s'impose de recherche entre tous les systèmes du fait du potentiel de croisement entre le terrorisme et la criminalité générale, soit les individus commettant des fraudes ou des délits de vol de valeur élevée pour spécifiquement financer les activités terroristes, etc. *Dans l'idéal, ils devraient aussi assurer l'interopérabilité avec les applications biométriques de contrôle des frontières si le droit national le permet.*

À l'échelon international, la police peut échanger des données biométriques selon des accords bilatéraux, multilatéraux ou régionaux mais la seule méthode globale officielle passe par l'Organisation internationale de police criminelle (OIPC plus communément connue sous le nom INTERPOL) qui facilite la coopération policière internationale. Il convient de noter que les pays contribuant par leurs données aux bases de données d'INTERPOL :

1. *demeurent propriétaire de leurs données* et peuvent obtenir leur retrait des bases de données à tout moment (voir Section 3.3.2. Recherches unidirectionnelles).
2. *déterminent la portée des données recherchées*, soit les données de recherche et les données consignées ne sont pas exposées aux données biométriques de pays désignés.

INTERPOL compte trois bases de données biométriques exploitables par ses 190 pays membres :

Visage – Elle offre les fonctionnalités suivantes :

- Identification des fugitifs et des personnes disparues
- Identification des personnes d'intérêt inconnues
- Identification de sujets d'images des medias publics
- Vérification d'images d'identité judiciaire reçues comparées à une base de données (1:n).

Empreintes digitales – Passerelle AFIS. Avec ce système, les responsables des forces de l'ordre des pays membres accèdent à distance à la base de données et reçoivent une réponse automatisée via le réseau de communications global sécurisé I-24/7 d'INTERPOL. La base de données contient des

Données de référence (empreintes de doigt et de paume) et des Données de scène de crime (marques de doigt et de paume).

ADN – Passerelle ADN (fonctionnant de manière similaire à la passerelle AFIS). INTERPOL a convenu de règles de traitement des données ADN avec tous ses pays membres et la base de données comporte quatre sections :

- scènes de crime non résolues
- délinquants connus
- personnes disparues
- restes humains non identifiés

INTERPOL offre aussi les services de son système de correspondance bilatéral d'ADN qui propose une plateforme privée pour les recherches et comparaisons d'ADN entre deux pays. L'entente repose sur une confiance partagée, une stratégie policière, des législations compatibles et des critères de correspondance convenus mutuellement, ainsi un nombre minimum de loci. Les profils ADN sont sélectionnés par chaque pays et envoyés de manière sécurisée à INTERPOL. Toute correspondance est notifiée aux deux partenaires et les données sont ensuite effacées du système. Les pays peuvent employer cet outil pour les comparaisons ponctuelles ou dans le cadre de leurs opérations régulières de correspondance.

Une fonction importante des Bases de données biométriques d'INTERPOL est la collecte des données biométriques des combattants terroristes étrangers et autres terroristes pour empêcher leurs mouvements transfrontaliers. Elle contribue au Flux d'action de la Stratégie de lutte contre le terrorisme globale d'INTERPOL qui priorise l'identification des membres de groupes terroristes transnationaux.

3.1.3 Bases de données biométriques d'INTERPOL : Supervision et gouvernance

La gouvernance interne et l'exploitation des bases de données biométriques d'INTERPOL sont supervisées par la Commission de contrôle des fichiers d'INTERPOL (CCF), un organisme indépendant. Elle assume trois fonctions :

1. assurer que le traitement des données à caractère personnel par INTERPOL est en conformité avec la réglementation de l'organisation
2. conseiller INTERPOL sur tout sujet impliquant le traitement des données à caractère personnel
3. traiter les demandes concernant les informations contenues dans les fichiers de l'organisation.

La CCF est devenue un organisme officiel de l'organisation lorsque la 77e Assemblée Générale a voté en 2008 pour renforcer son statut en amendant les Statuts afin d'intégrer la CCF dans sa structure juridique interne. En novembre 2016, l'Assemblée Générale d'INTERPOL a adopté un ensemble de réformes portant sur les mécanismes de supervision d'INTERPOL. Il incluait l'adoption du nouveau Statut de la CCF, réformant en profondeur sa composition, sa structure et ses procédures. Ce nouveau cadre de travail juridique est entré en vigueur le 11 mars 2017 pour renforcer les fonctions de supervision et de conseil de la Commission tout en rehaussant sa capacité à offrir une voie de recours efficace aux individus pour les données les concernant susceptibles d'être traitées dans les fichiers d'INTERPOL.

3.1.4 Gestion des données de listes de surveillance biométriques et biographiques

Les listes de surveillance sont une forme de système d'alerte reposant sur une diversité de données, exploitées au niveau national, parfois régional. Elles sont censées offrir des avertissements anticipés et des procédures de contrôle pour faciliter la reconnaissance et l'identification des criminels et terroristes ainsi que des marchandises et matières suspectes aux points de franchissement des frontières. Les listes de surveillance sont de différents types, notamment :

- *Listes de surveillance biographiques :* informations sur les personnes disparues ou recherchées, les personnes d'intérêt, les interdictions de vol, etc.
- *Listes de surveillance biométriques :* les modalités communes incluent les empreintes digitales, les images faciales et l'iris (L'ADN n'est pas actuellement communément employé) et présentent des fonctionnalités similaires avec les listes de surveillance biographiques, soit les personnes disparues ou recherchées, les personnes d'intérêt, les terroristes soupçonnés ou connus, etc.
- *Listes de surveillance contenant des informations sur les marchandises et documents :* véhicules volés, documents de voyage perdus et volés[61], objets d'art volés, etc.
- *Listes de surveillance contenant des informations sur le modus operandi ou la reconnaissance des substances dangereuses :* la méthode spécifique employée pour perpétrer un crime ou une série de crimes, de nouvelles méthodes de reconnaissance de la fausse monnaie ou des documents de voyage falsifiés, des méthodes et des composants chimiques utilisés pour la fabrication de substances illicites, etc.

Les listes de surveillance servent aussi aux organismes de maintien de l'ordre internationaux et régionaux comme INTERPOL[62] et EUROPOL[63] et aux organisations autres que les forces de l'ordre pour des applications dont les résultats couvrent un éventail ample et diversifié d'utilisateurs :

- *Forces de l'ordre :*
  - International[64] ; INTERPOL[65].
  - Régional : EUROPOL[66] et autres organisations régionales
  - National[67] : Police, Immigration, Douanes, etc.
- *Organisations internationales*
  - Nations Unies (NU,[68]) etc.
- *Organisations publiques*,
  - Autorités de délivrance des passeports,[69] Autorités de délivrance des permis de conduire, etc.
- *Organisations privées /commerciales,*
  - Compagnies aériennes, compagnies d'assurance, producteurs alimentaires, etc.

[61] Voir : https://www.interpol.int/INTERPOL-expertise/I-Checkit
[62] Voir : https://www.interpol.int/
[63] Voir : https://www.europol.europa.eu/
[64] Voir : ICAO TRIP Guide on Border Control Management, version 1, chapitre : 5-M
[65] Voir : https://www.interpol.int/INTERPOL-expertise/Databases
[66] Voir : https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
[67] Voir : ICAO TRIP Guide on Border Control Management, version 1, chapitre : 4-E
[68] Voir : https://www.un.org/sc/ctc/
[69] Voir : https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

Les organisations autres que les forces de l'ordre utilisent les listes de surveillance dans leurs domaine de responsabilité ou d'activité propre afin de protéger leurs produits et processus et d'éviter les actions frauduleuses.

3.2 Limitations des listes de surveillance biographiques

En majorité, les listes de surveillance des forces de l'ordre sont basées sur des informations biographiques individuelles, soit les noms, date de naissance, etc. Ces informations peuvent ne pas être fiables et sujettes à l'erreur ou au changement. Parmi les exemples communs, nous relevons :

- noms incorrectement traduits ou orthographiés
- usage d'un alias ou surnom au lieu du nom officiel mentionné dans le document de voyage
- date de naissance erronée ou séquence des chiffres incorrecte, soit 12/01/1967 au lieu de 01/12/1967
- binationaux
- changement de nom et obtention d'un nouveau document de voyage ou d'une nouvelle identité
- présentation de document de voyage falsifié, contrefait ou obtenu de manière frauduleuse sous un ou d'autres noms
- présentation de document de voyage authentique mais d'une autre personne pour usurper l'identité du titulaire d'origine
- « partage » d'un document de voyage avec quiconque utilisant une photographie 'morphée', soit une image mêlant deux visages différents (voir Section 2.3.2.)
- jumeaux ou triplés échangeant leurs identités ou documents de voyage

L'identification positive du sujet est dès lors primordiale, entraînant la création de listes de surveillance biométriques.

3.3 Listes de surveillance biométriques

Les listes de surveillance biométriques assument un rôle additionnel pour les processus de vérification biométrique 1:1 se déroulant aux frontières. Le contrôle de vérification 1:1 (voir Section 3.1) exploite les données biométriques enregistrées dans la puce du document de voyage électronique pour authentifier l'identité de la personne se présentant à la frontière. Le concept de liste de surveillance franchit une étape additionnelle et offre une capacité de recherche 1:n (un sur plusieurs) pour vérifier les données biométriques du voyageur dans une base de données biométriques de personnes d'intérêt. Un équipement d'enregistrement biométrique similaire est nécessaire pour les deux processus mais la base de données nécessite un logiciel de recherche 1:n ainsi qu'un logiciel de correspondance 1:1 afin de pouvoir exécuter l'une des tâches ou les deux, selon les besoins. De là un impératif d'investissement additionnel. L'efficacité de la recherche 1:n dans une liste de surveillance dépend des facteurs suivants :

- qualité des données d'enregistrement
- type de données stockées dans la base de données
- performances du système (voir Section 1.1)
- vulnérabilité du système aux attaques de présentation exploitant des techniques comme la morphose ou l'usurpation (voir Section 2.2)

Parmi les exemples de grandes listes de surveillance internationales et régionales, nous relevons :

I-24/7 d'INTERPOL - Toutes les bases de données d'INTERPOL, sauf le Réseau d'information balistique d'INTERPOL (IBIN - INTERPOL Ballistics Information Network), sont accessibles en temps réel via le réseau I-24/7 qui connecte tous les Bureaux centraux nationaux (NCB - National Central Bureaus) d'INTERPOL. Il est relié au système de notices d'INTERPOL afin d'émettre des alertes internationales sur les fugitifs, suspects de crimes, personnes liées ou d'intérêt pour des enquêtes criminelles en cours, personnes et entités soumises à des sanctions du Conseil de sécurité des NU, menaces potentielles, personnes disparues et cadavres.

SIE (Système d'information EUROPOL) EUROPOL - Cette base de données contient les informations criminelles et de renseignement couvrant tous les domaines criminels sous le mandat d'EUROPOL, notamment le terrorisme.

Étude de cas 8 – ETIAS

La Commission de l'Union Européenne propose la création d'un Système européen d'information et d'autorisation concernant les voyages (ETIAS - European Travel Information and Authorisation System)[70] afin de renforcer la sécurité des déplacements dans l'espace Schengen selon des accords d'exemption de visa. La liste de surveillance de l'ETIAS, créée et gérée par EUROPOL, doit intégrer les données liées à des personnes soupçonnées d'avoir commis ou pris part à des infractions criminelles ou de personnes à l'encontre desquelles des indications factuelles ou des motifs raisonnables permettent de penser qu'elles ont commis des infractions criminelles.
La liste de surveillance doit être créée sur les bases suivantes :

1) Liste du Comité des sanctions des Nations Unies
2) Informations liées aux crimes terroristes ou autres infractions criminelles graves procurées par les États membres
3) Informations liées aux crimes terroristes ou autres infractions criminelles graves obtenues dans le cadre de la coopération internationale

3.3.1 Avantages des applications biométriques de lutte contre le terrorisme

3.3.1.1 À l'intérieur des frontières nationales

Les bases de données biométriques ont joué un rôle toujours plus important dans les enquêtes criminelles depuis le développement des premiers systèmes de classification et de recherche des empreintes digitales dans les années 1890. L'informatisation et les avancées scientifiques et technologiques du 20e siècle ont grandement accru l'efficience et la puissance de traitement de ces systèmes et ouvert l'éventail des modalités disponibles, ainsi le visage, l'ADN, la voix, etc. Les systèmes de recherche biométrique employés par nombre d'organismes des forces de l'ordre offrent de nos jours des algorithmes complexes avancés susceptibles de faciliter une recherche rapide et exacte parmi de grands volumes de données. Cependant, le grand avantage présenté par une recherche dans une base de données de détection de crime sur la plupart des autres processus de collecte de renseignements et d'enquêtes repose sur le fait qu'elle offre une surveillance continue 24 heures sur 24, chaque jour de l'année, tant que les données sont conservées dans la base de données.

[70] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

Une correspondance est identifiée dès lors que les données sont enregistrées et interrogées, dans la mesure où les données correspondantes sont déjà dans la base de données, ou si les données sont consignées dans le système pour générer une correspondance des semaines, des mois, des années ou même des décennies plus tard. Par conséquent, une recherche dans une base de données de détection de crime est considérée comme l'un des atouts les plus rentables et constamment utiles des enquêteurs et des analystes du renseignement modernes. Les bases de données peuvent aussi être

1. combinées à l'échelon national pour assurer une couverture efficace d'un pays, indépendamment de sa taille physique et de sa population relative
2. rendues interopérables avec des systèmes biométriques aux frontières et
3. liées à des bases de données biométriques internationales ou autrement pertinentes.

Enquête criminalistique en temps réel

Les organismes de maintien de l'ordre de nombre de pays ont développé et exploité cette technologie biométrique afin d'établir l'identité des auteurs de crimes et de confirmer leurs antécédents criminels, d'inculper ou de disculper des suspects de leur implication dans des crimes et délits connexes. Ces bases de données se sont avérées particulièrement précieuses pour les enquêtes sur le terrorisme et leur contribution a été rehaussée ces dernières années par l'avenue des 'Enquêtes criminalistiques en temps réel'. Ce processus exploite la récupération et la génération rapide de données criminalistiques interrogeables des scènes de crime comme les images faciales récupérées sur des dispositifs électroniques ou des photographies, des échantillons d'ADN rapidement profilés ou la transmission électronique d'images numériques de marques de doigt sur une scène de crime directement dans un AFIS pour une recherche instantanée. Il est désormais possible et devient chaque jour plus routinier d'interroger et de comparer du matériel biométrique significativement probant pendant le déroulement de l'examen d'une scène de crime. De là un potentiel de génération de renseignements criminalistiques susceptibles d'aboutir à l'identification rapide d'un suspect ou de modifier pour les enquêteurs les lignes dynamiques d'une enquête qui débute. Pour les enquêtes sur le terrorisme, de nouveaux suspects ou leurs associés peuvent être identifiés juste après un incident afin d'éviter de nouvelles attaques. Évidemment, cette capacité est parachevée si l'ensemble des données biométriques interrogées en temps réel est aussi vaste que possible.

Les bases de données sont très utiles pour gérer la suite immédiate des 'attentats suicides à la bombe' alors que les restes physiques du poseur de bombe peuvent être mêlés à ceux des victimes. Dans ces situations, il est impératif de déterminer dans l'urgence à la fois l'identité du poseur de bombe, pour faire avancer l'enquête et éviter de nouvelles attaques, et celle des victimes au nom de leurs familles. ADN, empreintes digitales et odontologie (dentisterie criminalistique) sont les principales données biométriques exploitées car ce sont les principaux identificateurs employés pour l'Identification des victimes de catastrophe[71].

3.3.1.2 Entre des frontières nationales

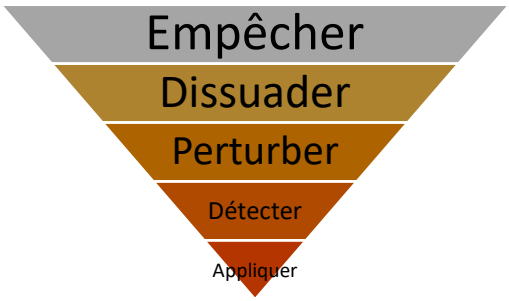
Ainsi que mentionné auparavant, les interventions biométriques aux frontières relèvent de deux catégories :

[71] L'Identification des victimes de catastrophe (IVC) est une procédure reconnue internationalement de récupération et d'identification des victimes d'un incident mortel de grande ampleur et de soutien des personnes endeuillées durant le processus. Elle est assurée par le personnel des forces de l'ordre alors que les processus sont convenus à l'échelon international dans le cadre de l'appartenance aux comités IVC d'INTERPOL. INTERPOL peut aussi procurer une assistance et une coordination directes dans le cas des incidents internationaux complexes de grande ampleur.

(1) *Vérification d'identité biométrique (1:1)* – la comparaison des données biométriques obtenues d'un voyageur à la frontière avec des données biométriques, ainsi celles stockées dans le document de voyage comme un passeport électronique.
(2) *Recherche de liste de surveillance biométrique (1:n)* – la recherche de données biométriques obtenues à la frontière ou dans un passeport électronique ou des documents de voyage dans une liste de surveillance contenant les données biométriques de personnes d'intérêt comme les individus recherchés par les forces de l'ordre, des terroristes connus ou soupçonnés, etc.

Chaque processus améliorer l'appréciation du risque des voyageurs via la gestion de l'identité.[72] Le fait de disposer des deux processus en exploitation au passage de la frontière constitue la configuration optimum. La Vérification d'identité à la frontière confirme l'identité du voyageur selon des données biométriques enregistrées et authentifiées alors qu'une Recherche de liste de surveillance biométrique peut révéler que cette identité confirmée est celle d'une personne d'intérêt. Cette approche exige des investissements accrus mais procure des niveaux supérieurs d'assurance et de sécurité qui justifient normalement les dépenses additionnelles.

Figure 5 - Adaptation d'*ICAO TRIP Guide on Border Control Management, Montréal (2018)*
(Avec la permission de l'OACI)



Organismes aux frontières	Empêcher, dissuader et perturber le voyage	Listes de surveillance Renseignement sur les voyages
Organismes de maintien de l'ordre et de sécurité	Enquêter, détecter et faire appliquer	• Enquêtes sur scène de crime • Renseignement criminel et de sécurité

Les listes de surveillance peuvent varier de par leur taille et la complexité de leur contenu. Certaines listes de surveillance biométriques comprennent des bases de données distinctes de données de référence obtenues de certaines catégories de personnes d'intérêt. D'autres listes de surveillance biométriques peuvent ajouter une sélection de données biométriques de scène de crime pour étendre leur portée. Néanmoins, l'interprétation la plus large du concept de liste de surveillance aboutirait à une intégration juridique de l'ensemble des bases de données biométriques des forces de l'ordre à l'échelon national (voir Section 3.3.2) au sein d'une configuration de 'liste de surveillance nationale' comme illustré en Fig. 5. Dès lors, une quantité optimale de données pertinentes serait exposée à des recherches sur des listes de surveillance pour assurer une protection maximale des voyageurs et de la sécurité de la nation. Cependant, certaines contraintes légales et réglementaires nationales risquent d'empêcher une telle solution.

3.3.1.3 Au-delà des frontières nationales

Un pays peut compter sur des actifs à l'étranger considérés comme vulnérables à des attaques terroristes. La biométrie peut former une part essentielle d'un plan d'atténuation des menaces. Par

[72] Voir l'ICAO TRIP Guide on Border Control Management, Montréal (2018) pour en savoir plus.

exemple, ce peut être un impératif pour filtrer les employés du pays hôte travaillant sur des sites relevant du pays d'origine, ainsi une ambassade. Une coopération pourrait ici s'avérer nécessaire entre les deux pays et, dans l'idéal, un accord juridique de recherche de données biométriques et biographiques dans les bases de données des deux pays afin de déterminer qu'un employé n'a pas d'antécédents criminels ou une connexion notoire avec le terrorisme dans l'un ou l'autre pays. De même, si des nationaux du pays hôte sont liés au terrorisme dans le pays d'origine, les deux pays bénéficieraient d'un échange et de recherches des données biométriques entre eux, d'abord afin de protéger les actifs à l'étranger du pays d'origine, ainsi les entreprises commerciales, installations diplomatiques, activités et autres, mais aussi pour aider le pays hôte à identifier et gérer le retour de ses nationaux soupçonnés d'activités terroristes. Cette forme de coopération bilatérale et d'autres options d'échange de données sont exposées en Section 3.3.2.

3.3.1.4 Biométrie de source militaire

Certains pays emploient leurs forces militaires pour combattre le terrorisme au sein de leurs frontières nationales comme à l'étranger. Les données biométriques sont souvent employées durant ces déploiements pour nier leur anonymat aux terroristes qui peuvent chercher à se cacher et se mêler aux populations locales afin d'éviter toute détection, voire les exploiter comme des 'boucliers humains'. Les forces militaires utilisent des techniques similaires à celles des organismes de maintien de l'ordre, ainsi le déploiement de dispositifs mobiles ou statiques de capture biométrique pour obtenir des échantillons de référence de terroristes soupçonnés ou l'examen criminalistique d'éléments récupérés sur des détenus ou dans des lieux d'intérêt connectés à des activités terroristes ou insurrectionnelles.

Les données biométriques obtenues de ces opérations militaires peuvent s'avérer aussi précieuses pour les organismes de maintien de l'ordre en connexion avec les enquêtes de lutte contre le terrorisme. Cependant, des contraintes substantielles au partage et à l'usage de ces données sont possibles, dépendant grandement des aspects suivants :

- autorité légale d'échange de ces données biométriques en conformité avec le droit national et le droit international des droits de l'homme
- admissibilité des données biométriques militaires et autres preuves devant les tribunaux civils
- compatibilité des normes de qualité de la science biométrique et criminalistique militaire avec celles employées par les autorités civiles du pays concerné.

Dès lors, même si l'échange de données peut être légal, il risque de ne pas respecter les exigences normatives juridiques d'admissibilité en tant que preuves, sans pour autant perdre sa valeur significative pour le renseignement (voir Section 3.3.3.).

Étude de cas 9 – Terrorist Explosive Device Analytical Centre

Le TEDAC (Terrorist Explosive Device Analytical Centre - Centre d'analyse des dispositifs explosifs terroristes) du FBI aux États-Unis est un exemple de ce type de capacité. Le TEDAC coordonne les efforts de l'ensemble du Gouvernement, des forces de l'ordre au renseignement en passant par l'armée, pour collecter et partager des données criminalistiques et des renseignements sur les dispositifs, tactiques, techniques et procédures afin de désarmer et de mettre en échec les EEC (Engins Explosifs de Circonstance), de les associer à leurs créateurs et, plus important, d'éviter les attaques futures. À ce jour, le TEDAC a reçu plus de 100 000 soumissions d'EEC de plus de 50 pays.

La BAU (Biometrics Analysis Unit - Unité d'analyse biométrique) contribue à la capacité globale du Gouvernement des États-Unis et de ses partenaires internationaux à contrecarrer et mettre en échec les menaces liées aux EEC grâce à un examen criminalistique haut de gamme en temps opportun des empreintes latentes et de l'ADN sur les matériaux des EEC, générant des renseignements actionnables à des fins d'enquête.

3.3.1.5 Protection mutuelle assurée

Les avantages des systèmes biométriques pour la surveillance et la détection des terroristes peuvent être pleinement exploités uniquement grâce à la coopération et au partage des données par les nations. Un pays peut disposer de systèmes biométriques nationaux complets et efficaces au sein et entre ses frontières et même appartenir à un réseau régional sophistiqué mais être dépourvu d'accès à des données sur les terroristes d'autres pays hors de son réseau national et régional et demeurer dès lors potentiellement vulnérable. Le partage national, bilatéral et régional des données (voir Section 3.3.2.) propose une solution partielle. Cependant, il est impératif que les données biométriques des terroristes soient partagées à l'échelon international, globalement, afin d'assurer la protection mutuelle de toutes les nations. Il devient dès lors possible de dissuader et de mettre en échec les terroristes qui peuvent trouver leurs bases temporairement dans des pays avec pas ou peu de capacités biométriques et ainsi adopter de nouvelles identités ou obtenir des documents de voyage de nature frauduleuse pour ensuite voyager incognito vers d'autres destinations. Un système complet et rigoureux de partage international de données biométriques doit être créé pour contrecarrer ces tactiques et refuser aux terroristes leur anonymat ou des sanctuaires depuis lesquels opérer.

Les bases de données biométriques d'INTERPOL constituent un bon exemple de ce type de capacité globale. Elles sont conçues pour assumer cette fonction vitale de protection en permettant aux nations de partager leurs données biométriques liées au terrorisme et, plus important, sont soumises à des procédures de gouvernance bénéficiant d'un accord international et soumises à une supervision indépendante.

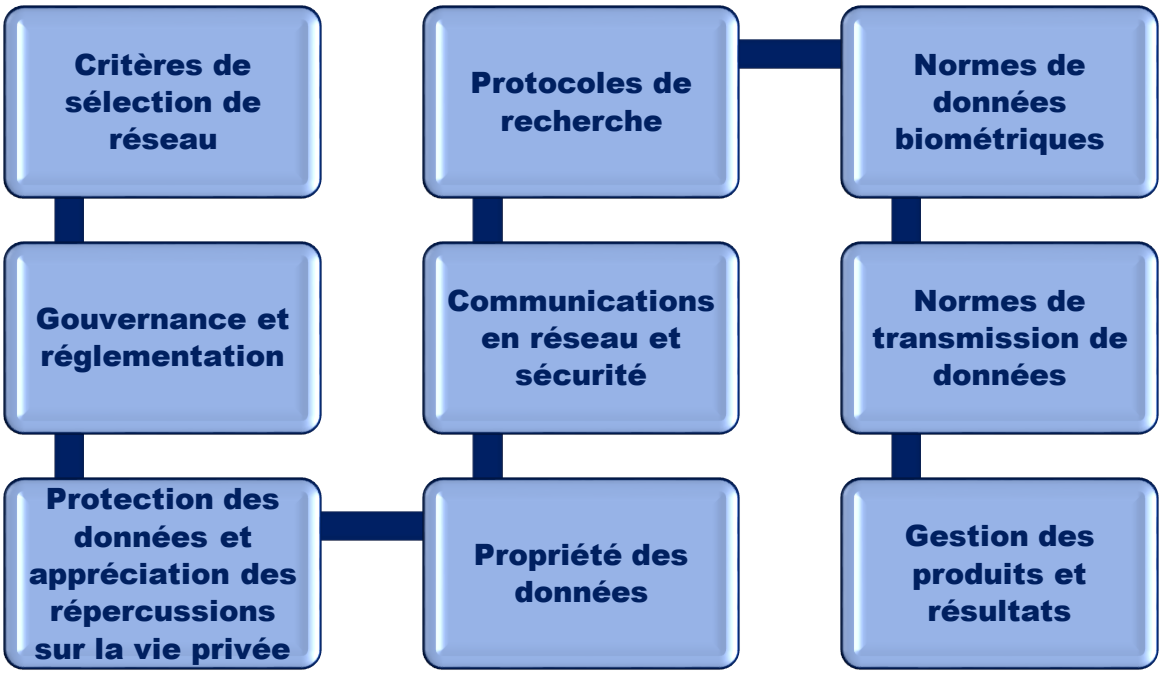
La Figure 6 illustre l'ample éventail de sources de données biométriques *potentielles*, détenues par des organisations publiques nationales et internationales, susceptibles d'être exploitées à des fins de lutte contre le terrorisme. Les listes ne sont pas exhaustives et l'accès à l'une quelconque de ces bases de données est, bien entendu, soumis à des contraintes légales et réglementaires nationales. Néanmoins, c'est la manifestation de la capacité des données biométriques à être connectées, en théorie, afin de procurer une protection mutuelle contre la menace terroriste en termes de portée nationale, régionale et globale.

Figure 6 - Sources de données biométriques

3.3.2 Protocoles de partage des données et Intégration légale des bases de données

Traditionnellement, les bases de données biométriques des forces de l'ordre étaient exploitées sous forme de systèmes autonomes. En effet, chaque application servait un besoin distinct et séparé d'une activité et aucun avantage n'était perçu en termes de partage des données entre ces systèmes. Ces bases de données étaient spécifiquement conçues pour les fonctions des activités associées à la police, à la gestion des frontières ou au système carcéral. Cependant, les menaces croissantes du terrorisme global, ces dernières décennies, ont forcé nombre de gouvernements à réévaluer la manière dont leurs bases de données sont employées et comment ils pourraient partager des données entre eux pour procurer un surcroît de protection à leurs citoyens. De là une connectivité et une interopérabilité accrues entre les bases de données à l'échelon national et le développement de réseaux bilatéraux, multilatéraux et régionaux de bases de données à l'échelon international. Tout a commencé par l'agrégation de bases de données disparates et monomodales pour évoluer, dans certains pays et régions, sous forme de réseaux de remplacement de pointe, proposant des bases de données multimodales interconnectées, conçues pour servir une palette de besoins d'activité des fonctions de maintien de l'ordre, de gestion des frontières et autres de nature gouvernementale, aux échelons national et international. Les exigences de ce type de connectivité sont les suivantes :

Figure 7 – Exigences de connectivité de réseau biométrique



Critères de sélection de réseau – Les propriétaires de données biométriques devraient évaluer leur adhésion à un réseau biométrique non seulement en termes de leurs propres besoins d'activité et objectifs opérationnels, quelle que soit leur importance, mais aussi selon une perspective élargie tenant compte de la valeur ajoutée potentielle pour leur pays ou leur région ainsi que pour leurs autres partenaires du réseau. Cette approche est essentielle et fondamentale pour le développement de bases de données biométriques de lutte contre le terrorisme en réseau. Il est aussi improbable que les propriétaires de données cherchant à intégrer un réseau international se risquent à partager leurs données avec des partenaires peu fiables ou scrupuleux, ces préoccupations devant être gérées correctement par tout réseau comptant de nombreux membres internationaux, ainsi voir Section 3.1.2. Applications policières et INTERPOL.

Gouvernance et réglementation – Les réseaux biométriques doivent fonctionner selon un cadre juridique permettant le transfert de données biométriques et autres métadonnées associées. Chaque base de données existante devrait déjà être en exploitation selon les droits nationaux et le droit international des droits de l'homme bien qu'un complément législatif puisse s'avérer nécessaire afin d'autoriser les recherches entre différentes bases de données dans un pays ou internationalement. Pour les réseaux internationaux, cela passe normalement par des accords formalisés ainsi des Mémorandums d'entente, entre les entités ou pays participants. Une recherche légale peut être limitée à des recherches uniques déclenchées au cas par cas (ainsi pour des délits spécifiés) ou appliquée plus largement, comme une recherche automatique de toutes les données enregistrées d'un réseau.

Un cadre réglementaire devrait prévoir une supervision indépendante de l'intégralité du réseau et prêter particulièrement attention aux fonctions de gestion des données ainsi qu'aux fins pour lesquelles les données doivent être employées pour éviter ainsi toute extension de la portée sans autorisation, par exemple les recherches d'ensembles de données dans ou hors du réseau qui sont

interdits par le droit ou les protocoles de fonctionnement en vigueur. Certains pays ont nommé des responsables publics pour assumer cette fonction, ainsi des régulateurs ou des commissaires des données biométriques. En outre, d'autres autorités de régulation, comme le Forensic Science Regulator au Royaume-Uni, sont chargées de la supervision des processus scientifiques, notamment ceux utilisés pour créer les profils et données biométriques criminalistiques exploités dans ces bases de données. En d'autres termes, l'exploitation de la base de données et des données biométriques criminalistiques qu'elle contient est soumise à une surveillance et une supervision indépendantes, incluant le travail de comités d'examens éthiques ou d'organismes similaires. (voir Section 2.1.1.)

Protection des données et appréciation des répercussions sur la vie privée - (soir Sections 2.2.3. et 2.2.4.).

Propriété des données – Chaque enregistrement biométrique doit disposer d'un propriétaire des données défini (voir Section 2.2.6.) qui assume la responsabilité, dans le cadre de la loi, pour l'enregistrement, l'usage, la conservation et la suppression des données. Cet aspect est particulièrement important pour gérer un réseau de bases de données biométriques contenant des volumes conséquents de données de sources diverses.

Communications en réseau et sécurité – Le flux de données biométriques et autres informations doit être efficient et opportun. Le réseau doit être sécurisé du fait de la nature des données qu'il renferme et offrir des niveaux appropriés de sécurité pour protéger les environnements d'exploitation, notamment les données, le matériel, les logiciels et le réseau de communication. Une bonne pratique consiste à conserver uniquement les données biométriques dans le système du réseau. Les données biographiques à caractère personnel liées à leurs données biométriques spécifiques devraient être consignées dans un système séparé. Cette mesure de protection évite l'accès à des informations personnelles et à des données biométriques depuis une seule et même application. Les données biométriques correspondent donc habituellement à un simple numéro de référence unique qui peut être lié aux données biographiques lui correspondant selon des procédures opérationnelles sécurisées, si besoin est.

Protocoles de recherche – Le réseau doit disposer de protocoles de consignation et de files d'attente de recherche systématiques et synchronisées qui contrôlent la durée et la séquence de chaque recherche pour assurer son exposition à l'ensemble de données intégral de chaque base de données du réseau afin de ne rien manquer même en cas de pic de fréquentation (voir paragraphe suivant - Bases de données biométriques en réseau : Protocoles de recherche).

Normes de données biométriques – Les recherches peuvent uniquement être exécutées en réseau si des données biométriques consignées par les partenaires sont de types compatibles. Par exemple, des chimies de profilage ADN différentes ont été employées dans le monde entier, ainsi dans le cas de l'Australie, de l'Europe et des États-Unis. Chacune de ces chimies a exploité un loci STR unique spécifique, outre le loci STR commun à toutes. Cependant, dans la mesure où le nombre de loci en commun était suffisant, il était possible de rechercher des profils selon ces différentes chimies dans l'une quelconque des bases de données ADN. Les chimies de profilage les plus récentes utilisent un nombre encore supérieur de loci STR de sorte que les loci communs à tous les partenaires sont proportionnellement plus nombreux.

Les normes techniques et scientifiques (ainsi ISO 17025) décrites en Section 2.4 devraient sous-tendre toutes les caractéristiques opérationnelles du réseau.

Normes de transmission de données – Une qualité insuffisante des images expose le réseau biométrique à des risques graves et inutiles comme le nombre accru de faux rejets, voire d'erreurs d'identification. Pour s'assurer que la qualité des images, ainsi le visage ou les empreintes digitales,

n'est pas dégradée durant la transmission entre réseaux, des normes doivent être mises en place[73] pour faire face aux exigences de résolution des images. En d'autres termes, l'image conserve une clarté et une définition identiques, indépendamment de l'endroit où elle est consultée dans le réseau.

Gestion des produits et résultats – Les correspondances de données biométriques produites par le réseau de recherche (produits) et les actions prises en résultante de ces correspondances (résultats) doivent être gérées prudemment et en conformité avec les impératifs légaux, des normes scientifiques rigoureuses et des protocoles organisationnels stricts (voir Section 3.3.3.). Les correspondances biométriques doivent être examinées par des pairs dans le cadre d'un Système de management de la qualité, par un autre expert (de préférence deux experts) avant la diffusion du résultat. Le risque d'une personne unique commettant une identification incorrecte est ainsi évité.

Bases de données biométriques en réseau : Protocoles de recherche - Deux méthodes fondamentales assurent la synchronisation des recherches entre des bases de données :

Recherche unidirectionnelle – Les données biométriques (a) sont enregistrées et interrogées dans la Base de données 1. Si aucune correspondance n'est identifiée, les données sont consignées dans la Base de données 1 et envoyées à la Base de données 2 pour une nouvelle recherche puis, à nouveau, en l'absence de correspondance, elles sont consignées dans la Base de données 2.

NB Des correspondances potentielles peuvent être manquées si les données (a) sont *uniquement* interrogées et *pas* consignées dans la Base de données 2 car le résultat de la recherche serait limité au moment exact de la recherche. Par exemple, si de nouvelles données de recherche (b), correspondant aux données biométriques (a), sont enregistrées et interrogées dans la Base de données 2 *après* le moment de la recherche des données (a), alors aucune correspondance n'est possible car les données (a) n'ont pas été consignées et, par conséquent, pas été exposées à la recherche de données (b). Dès lors, en cas de transferts unidirectionnels de données entre plusieurs bases de données, il est important que chaque base de données consigne les données après une recherche afin de s'assurer qu'elles sont discernées par les recherches suivantes pour ainsi préserver une couverture continue.

La gestion des données peut aussi s'avérer problématique en cas de transferts unidirectionnels, spécialement si les bases de données relèvent de juridictions ou de pays différents. Chaque propriétaire de données devrait rechercher un accord formalisé avec les autres partenaires pour la durée de conservation et la politique de suppression des données partagées. En l'absence d'un tel accord, les propriétaires des autres bases de données peuvent ne pas relever du même droit en regard de la base de données hôte, et donc ne pas être tenus d'obtempérer. Ils peuvent aussi être réticents à l'idée d'entreprendre les suppressions demandées pour d'autres raisons, ainsi les contraintes financières, de ressources ou de temps.

Recherche bidirectionnelle réciproque – Les données biométriques (a) sont enregistrées et interrogées dans la Base de données 1. Si aucune correspondance n'est identifiée, les données sont consignées dans la Base de données 1 et envoyées à la Base de données 2 pour une nouvelle recherche mais les données (a) ne sont pas conservées dans la Base de données 2. De même, si les données biométriques (b) sont enregistrées et interrogées dans la Base de données 2 puis renvoyées dans la Base de données 1 pour une nouvelle recherche, elles ne sont pas conservées dans la Base de données 1. Cette méthode est répliquée pour un nombre quelconque de bases de données du réseau car chaque base de données interroge ses nouveaux enregistrements de données via les autres bases de données. Le risque de manquer des correspondances potentielles (comme pour la recherche unidirectionnelle) est évité en consignant les données dans la base de données hôte *avant* la

[73] par ex. NIST Special Publication 1152 'Latent Interoperability Transmission Specification' www.nist.gov

recherche dans le réseau afin d'éviter les délais susceptibles autrement de permettre que des recherches en réseau concurrentes se manquent entre elles.

NB Ce système est souvent désigné comme une 'recherche de multiples enregistrements uniques' ou 'saisie unique et recherches multiples'. La base de données propriétaire des données les consigne après la recherche mais les autres bases de données exécutent uniquement une recherche. La gestion des données est ainsi simplifiée car les données du propriétaire sont stockées uniquement dans sa base de données ce qui réduit la quantité de données consignées dans le réseau. La séquence des recherches entre les bases de données doit être prudemment gérée, particulièrement si plusieurs bases de données d'une seule juridiction contribuent à une base de données d'une autre juridiction. Par exemple, les permutations de recherche entre les bases de données de la juridiction (1) doivent être complètement épuisées avant d'envoyer une quelconque recherche les concernant vers la juridiction (2). Dans le cas contraire, les correspondances peuvent être révélées dans la juridiction (2) alors qu'elles auraient dû apparaître déjà dans la juridiction (1). Pour l'éviter, il suffit d'envoyer les recherches de la juridiction (1) à la juridiction (2) via un conduit unique géré.

3.3.2.1 Données biométriques prédictives : L'usage proactif des réseaux de bases de données biométriques pour éviter les attaques terroristes

L'intégration des bases de données biométriques dans le vaste panorama du maintien de l'ordre et de la gestion des frontières (ainsi que des données biométriques militaires, le cas échéant) facilite l'analyse des produits collectifs du réseau, non seulement selon la perspective des besoins d'activité distincts, comme la détection des crimes, les contrôles d'identité à la frontière et autres, mais aussi sous forme de série bien plus étendue ou de motifs d'événements biométriques en eux-mêmes. En termes de menace terroriste, chaque événement affiche une pertinence directe ou indirecte ou peut sembler complètement inoffensif sans valeur apparente mais, une fois contextualisé avec d'autres informations ou événements biométriques, il peut contribuer significativement à une perception amplifiée du renseignement sur les mouvements et activités des terroristes. Certains de ces produits peuvent être plutôt explicites, ainsi la mise à jour de préparatifs de voyage suspects ou la révélation de liens avec des délits terroristes, mais d'autres peuvent être plus subtils et nuancés tout en demeurant des indicateurs précieux une fois considérés avec d'autres matériels pertinents. Illustrée en Figure 8 à la suite, cette méthode construit sur l'usage traditionnel, réactif et grandement passif des bases de données biométriques à des fins d'enquête et tente de sauver des vies en empêchant des attaques terroristes avant qu'elles ne surviennent en exploitant proactivement la biométrie d'un éventail le plus large possible de sources, conjointement avec d'autres produits de renseignement.

Figure 8 – Le modèle biométrique prédictif

Les bases de données biométriques traditionnelles (décrites en Section 1) ont été pensées pour être réactives et poser des questions d'enquête reposant sur l'identité et l'activité *actuelle* ou *passée*, ainsi *« Nous connaissons-vous ? Qui sont vos associés ? Qu'avez-vous fait ? »*. Les bases de données biométriques intégrées peuvent manifestement répondre aux même questions mais aussi servir de manière proactive afin d'inférer et de prédire des actions et associations potentielles futures, soit *« Que planifiez-vous avec vos associés ? Qu'allez-vous probablement faire ? Quand et où ? »*. Une analyse exhaustive et prudente de tous les produits dans tout le réseau s'avère donc essentielle et peut constituer un facteur de succès critique pour l'évaluation et l'anticipation de l'activité terroriste une fois associée à d'autres renseignements. C'est aussi le cas pour la gestion postérieure des résultats.

3.3.3 Gestion des résultats

3.3.3.1 Appréciation contextuelle des produits

Pour les systèmes biométriques autonomes, les produits peuvent être largement automatisés avec des interactions humaines minimes (voir Section 1). Toutefois, si les données contenues dans ces systèmes sont intégrées dans un réseau de bases de données biométriques multifonctions et recroisées, il est absolument vital que les produits soient examinés rigoureusement et compris avant d'entreprendre la moindre action. L'appréciation contextuelle de ces produits et des gestionnaires des résultats en découlant doit tenir compte des facteurs suivants :

Assurance d'une réponse proportionnée et gestion des identifications incorrectes ou collatérales – Il est naturel que les individus recevant et gérant les résultats d'un type quelconque de base de données biométrique, spécialement si elle est associée au terrorisme, forment des points de vue péjoratifs et partent du principe que quiconque identifié par le système doit être un terroriste. Néanmoins, ce n'est pas systématiquement le cas pour les raisons suivantes :

1. une erreur humaine ou du système peut identifier faussement un individu et, bien que cette occurrence soit rare, elle devrait former partie intégrante d'un protocole d'examen, particulièrement si d'autres données ou preuves semblent jeter le doute sur le résultat.
2. Les gouvernements et autres parties peuvent souhaiter abuser des produits biométriques en effectuant des fausses allégations d'activités terroristes afin de perturber leur opposition, les activistes politiques ou les militants des droits de l'homme (voir Section 2.2.5.)
3. la personne identifiée peut n'être aucunement impliquée dans un quelconque type d'activité terroriste. C'est pourquoi la valeur contextuelle et relative d'un quelconque résultat doit être correctement évaluée *avant* d'entreprendre une quelconque action.

Par exemple, un élément clé ou une localisation dans une enquête de terrorisme peut avoir été innocemment contaminé par une personne qui ne serait pas impliquée dans une quelconque activité terroriste ou par un membre négligent des forces de l'ordre. Le matériel criminalistique est ensuite recueilli par des experts en criminalistique et des enquêteurs sur la scène de crime et enregistré dans le réseau de bases de données approprié. Ces données criminalistiques 'collatérales' pourraient dès lors répondre à des recherches dans le cadre du réseau et générer une correspondance, ainsi lorsque l'individu fournit ensuite sa biométrie à une frontière. Les actions prises par ces autorités de gestion des frontières doivent donc reposer sur le contexte complet de toute correspondance biométrique et non sur une hypothèse automatique que la personne est un terroriste uniquement sur le fondement d'une correspondance biométrique. La réponse des organismes de maintien de l'ordre devrait être mesurée et proportionnée, en conformité avec le droit international des droits de l'homme. Ces procédures d'appréciation contextuelle doivent être soumises à une supervision rigoureuse et indépendante pour éviter toute détention erronée ou erreur judiciaire potentielle.

Stratégie de communication – Pour s'assurer que les appréciations contextuelles sont appliquées de manière cohérente et efficace dans la gestion des résultats, les autorités doivent définir des lignes de communication claires, sécurisées et ininterrompues entre les personnes évaluant les produits biométriques et le personnel opérationnel de première ligne ainsi que les décisionnaires devant agir sur la base des informations. Ceci implique la facilitation d'un dialogue urgent entre les propriétaires des données de scène de crime (un organisme de maintien de l'ordre) et les responsables du traitement d'un détenu en raison d'une correspondance avec des données de scène de crime. Un échange de ce type ou d'autres types d'informations est une occurrence plutôt régulière et normalement une procédure opérationnelle normalisée dans le domaine du maintien de l'ordre aux échelons nationaux et internationaux. Le réseau de communication doit aussi prioriser les résultats

des bases de données et opérer selon des délais convenus, spécialement dans le cas des personnes arrêtées ou détenues du fait d'une correspondance biométrique. La stratégie de communication doit également énoncer une liste complète de bénéficiaires des produits biométriques du réseau et mettre en place des critères de désamorçage des conflits pour éviter ou résoudre les litiges entre deux bénéficiaires sur des questions comme la primauté juridictionnelle ou les priorités d'enquête.

Modalités, normes de signalement des données de renseignement criminalistiques et interprétation scientifique – Certains réseaux de bases de données biométriques peuvent utiliser uniquement une seule modalité. Cependant, il plus habituel et efficace de compter sur une palette de modalités exploitées en parallèle au sein du réseau biométrique, ainsi les empreintes digitales, l'ADN et le visage. Les produits des systèmes multimodaux offrent le point de vue le plus étendu de l'activité en cas de combinaison avec des systèmes multifonction renfermant des données de renseignement criminalistique de scènes de crime mais aussi des données de référence d'une diversité de sources. Le matériel criminalistique récupéré sur une scène de crime peut ne pas toujours offrir une correspondance 'intégrale' avec des données de référence du fait des facteurs décrits en Section 1 mais se révéler tout de même d'une valeur probante immense pour une enquête. Ces deux composants doivent être pleinement appréciés et compris par les personnes chargées de la compilation des produits de base de données. La force relative de la correspondance et sa valeur potentielle probante ou pour les enquêtes mais aussi d'autres informations pertinentes obtenues durant l'appréciation contextuelle devraient être compilées et déclarées à un responsable public, un enquêteur ou un expert afin de pouvoir prendre des mesures appropriées et proportionnées. L'enregistrement des seules données susceptibles d'être produites en tant que preuves devant un tribunal s'avère donc une bonne pratique. De là la sécurité que toutes les correspondances pourront être pleinement exploitées dans le cadre d'une enquête ou révélées et produites devant un tribunal.

Étude de cas 10 - Procédures de gouvernance des notices d'INTERPOL
Un exemple opérationnel de gestion des échanges de données internationaux

Bien que le système de Notice rouge d'INTERPOL ne porte pas sur les résultats biométriques, il présente des parallèles solides avec les processus d'appréciation en Section 3.3.3.1. et procure un modèle stable de gestion des données à l'échelon global. Il est tenu d'opérer conformément avec la règle du droit international et les règles de l'organisation et d'assurer la facilitation d'une communication efficace entre les parties clés mais aussi la présence d'un système de traitement indépendant et rigoureux des réclamations et appels des sujets des procédures de Notice rouge.

Une Notice rouge est une demande par le Secrétariat général d'arrestation provisoire d'un individu dans l'attente d'une extradition sur requête d'un pays membre sur la base d'un mandat d'arrêt national valide. Une Notice rouge peut aussi être délivrée sur requête de tribunaux internationaux.

Outre les Notices rouges, INTERPOL délivre d'autres types de notices, ainsi la notice bleue qui est délivrée sur requête d'un pays membre afin d'obtenir des informations dans le contexte d'une enquête criminelle. Les pays membres peuvent aussi délivrer des diffusions, soit des requêtes de coopération circulant directement entre les pays membres.
INTERPOL ne peut pas insister, ni obliger un quelconque pays membre à arrêter un individu objet d'une notice rouge. INTERPOL ne peut pas non plus exiger d'un pays membre qu'il prenne une quelconque mesure en réponse à une requête d'un autre pays membre. Chaque pays membre d'INTERPOL décide par lui-même de la valeur juridique accordée à une Notice rouge au sein de ses frontières. En décidant d'agir sur une notice ou une quelconque autre requête, un pays assume la

pleine requête de la décision. L'efficacité opérationnelle des accords de notice rouge dépend de la capacité de gestion des références entre les National Central Bureau (NCB) sur une base 24/7/365.

Toutes les notices et diffusions doivent respecter les règles d'INTERPOL et la réglementation. Il s'agit ici notamment de l'Article 2 des Statuts d'INTERPOL qui fait explicitement référence à l'esprit de la Déclaration universelle des droits de l'homme et de l'Article 3 des Statuts d'INTERPOL selon lequel 'Toute activité ou intervention dans des questions ou affaires présentant un caractère politique, militaire, religieux ou racial est rigoureusement interdite à l'Organisation.'. Les règles d'INTERPOL relatives au traitement des données prévoient des critères additionnels de publication de chaque type de notice et l'affectation des responsabilités entre les diverses entités, soit le pays demandeur, le Secrétariat général, les pays destinataires, etc.

Supervision réglementaire - La conformité avec les règles d'INTERPOL est contrôlée à plusieurs niveaux. Le premier est constitué par les NCB qui envoient la requête de coopération policière (ainsi une demande de Notice rouge). Ils sont pleinement responsables de toute information qu'ils procurent pour les bases de données d'INTERPOL ou font circuler à l'aide du système d'informations d'INTERPOL. Ils doivent assurer que les informations sont exactes, pertinentes et actualisées et que leur traitement est en conformité avec les Statuts de l'organisation mais aussi avec leur législation nationale.
Le second niveau correspond au siège du Secrétariat général d'INTERPOL. En novembre 2016, le Secrétariat général a créé une cellule spécialisée dédiée comprenant une unité pluridisciplinaire de juristes, d'officiers de police, d'analystes et de spécialistes opérationnels pour examiner tous les niveaux de traitement des données, notamment en relation avec les Notices rouges et les diffusions. Toutes les requêtes sont examinées attentivement par la cellule spécialisée pour s'assurer qu'elles respectent les règles et Statuts d'INTERPOL. Dans le cadre de l'examen par la cellule spécialisée, des informations additionnelles de toutes les sources pertinentes peuvent être demandées afin de décider de la délivrance, ou non, d'une notice. En outre, un pays membre peut manifester ses inquiétudes relatives aux informations traitées par un autre pays membre, notamment la publication d'une Notice rouge, s'il considère que la procédure n'a pas respecté les règles d'INTERPOL.

Gestion des réfugiés - Depuis juin 2014, INTERPOL a mis en œuvre une nouvelle politique en relation avec les cas concernant les réfugiés. INTERPOL est ainsi en mesure d'assister des pays membres afin d'empêcher les criminels d'abuser du statut de réfugié tout en procurant des mesures de protection adéquates et efficaces afin de protéger les réfugiés authentiques. Chaque demande de diffusion et de Notice rouge à l'encontre d'un réfugié est appréciée par le Secrétariat général ou, le cas échéant, par la Commission de contrôle des fichiers d'INTERPOL (voir Section 3.1.2.), au cas par cas. En général, le traitement des diffusions et des Notices rouges à l'encontre des réfugiés n'est pas autorisé si le statut du réfugié ou du demandeur d'asile a été confirmé alors que la requête de notice /diffusion émane d'un pays où l'individu craint d'être persécuté.

Les droits des individus sujets d'une notice /diffusion - La décision de publication, ou non, d'une notice ou de consignation des informations dans les bases de données d'INTERPOL est sans effet sur les droits de l'individu, notamment son droit à la présomption d'innocence, son droit de contester les faits devant les autorités concernées du pays ayant délivré le mandat d'arrêt et recherché l'assistance d'INTERPOL ou son droit de contester les faits devant les autorités nationales chargées d'apprécier la demande d'extradition.
Un individu dispose au moins des trois options suivantes grâce auxquelles contester une Notice ou une diffusion :

- Défendre son cas devant les autorités nationales du pays demandeur, soit directement, soit par l'entremise d'une représentation juridique. Comme une notice rouge repose sur un mandat d'arrêt valide, si ledit mandat d'arrêt est retiré par les autorités compétentes nationales, la notice rouge est supprimée.
- Contacter la Commission de contrôle des fichiers d'INTERPOL.
- Demander à son propre pays d'assumer la défense lui-même et de contester la Notice rouge.

Si une diffusion ou une Notice rouge est annulée, quelle qu'en soit la raison, un message est envoyé à tous les pays membres les informant de la décision et leur demandant de retirer toutes les informations connexes de leurs bases de données nationales.

Ces mesures de protection assurent un processus transparent et structuré pour répondre à ces questions et les résoudre tout en évitant les abus potentiels des Notices rouges.

3.3.3.2 Objectifs stratégiques et lignes directrices des enquêteurs

Les stratégies nationales et régionales de lutte contre le terrorisme devraient refléter l'importance des données biométriques et de la criminalistique. Les organismes de maintien de l'ordre et de gestion des frontières devraient activement soutenir ces stratégies en employant l'ensemble des ressources criminalistiques et biométriques dont ils disposent et préserver des bases de données efficaces.

Des Stratégies criminalistiques et biométriques peuvent aussi être définies à l'échelon des enquêtes, une pratique à encourager par la formation et la doctrine opérationnelle. Le responsable en chef d'une enquête liée au terrorisme devrait énoncer les principaux objectifs criminalistiques et biométriques dès le début de l'enquête. Les caractéristiques biométriques devraient inclure habituellement :

- Tous les échantillons de référence biométriques des détenus, obtenus durant l'enquête, doivent être de qualité optimale.
- Toutes les scènes de crime doivent être soumises à des examens criminalistiques exhaustifs et parfaitement séquentiels pour maximiser le rendement de l'ADN et des empreintes digitales afin d'établir des associations terroristes étendues outre les exigences criminalistiques spécifiques de l'enquête.
- Toutes les données biométriques pertinentes récupérées durant l'enquête doivent être enregistrées ou interrogées dans toutes les bases de données nationales et internationales pertinentes.

Ces trois éléments de stratégie biométrique répondent aux aspects suivants :

1. *les besoins de l'enquête*, soit des données de référence biométriques de qualité supérieure pour une comparaison 1:1 efficace avec le matériel des scènes de crime ainsi que l'enregistrement et la recherche dans les bases de données pour faire avancer l'enquête et
2. *les exigences d'autres opérations de renseignement et enquêtes liées au terrorisme* en adoptant une perspective étendue des scènes de crime et en recueillant du matériel biométrique peut-être sans pertinence pour le cœur de l'enquête mais susceptible de révéler des associés inconnus, des cellules, des réseaux et
3. les données biométriques collectées lors d'une enquête peuvent non seulement aider à résoudre ou établir des liens avec d'autres enquêtes mais aussi potentiellement *empêcher des attaques terroristes futures* et, ce faisant, sauver des vies.

3.4 Pratiques recommandées

a) Les États devraient lutter contre la menace que constituent les déplacements continus de terroristes franchissant les frontières internationales en employant des systèmes biométriques de protection des frontières et des actifs nationaux et en partageant en toute légalité les données biométriques avec les partenaires internationaux.

b) La sécurité aux frontières peut être gérée plus efficacement en employant des techniques de vérification biométrique 1:1 combinées à des contrôles de listes de surveillance biométriques 1:n afin de suivre et de détecter les terroristes et leurs associés. Les listes de surveillance biométriques peuvent être créées à toute échelle à partir de collections de référence limitées grâce à une connectivité intégrale avec les bases de données de détection des crimes et de gestion de l'identité des forces de l'ordre, sous réserve des contraintes réglementaires et législatives nationales et du droit international des droits de l'homme.

c) Il est vivement recommandé aux États de maximiser leur usage des Bases de données biométriques d'INTERPOL (visage, empreintes digitales et ADN) afin de lutter contre la menace du terrorisme et des combattants terroristes étrangers.

d) Le partage des données biométriques au niveau international est un outil vital de la lutte contre le terrorisme mais doit respecter le droit international des droits de l'homme. Les gouvernements doivent s'assurer que le partage des données biométriques ne facilite pas des arrestations menant à la torture ou à l'imposition de la peine de mort.

e) Il est impératif que le contexte d'ensemble de toute correspondance biométrique fasse l'objet de recherches exhaustives avant d'entreprendre une action quelconque, dans le respect intégral du droit international des droits de l'homme.

f) Les stratégies nationales et régionales de lutte contre le terrorisme devraient refléter l'importance de la criminalistique et de la biométrie en imposant la responsabilité aux organismes de gestion des frontières et de maintien de l'ordre de maximiser leur collecte et leur usage légaux de matériel biométrique et criminalistique et de préservation de bases de données et de protocoles de partage des données efficaces.

3.4.1 Documents de référence

ICAO TRIP Guide on Border Control Management, Montréal (2018)

PNRGOV EDIFACT & XML Message Implementation Guide:
www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

WCO/IATA/ICAO Guidelines on PNR (Doc 9944)

OACI Doc 9303 — Machine Readable Travel Documents

www.interpol.int/INTERPOL-expertise/I-Checkit

www.interpol.int/INTERPOL-expertise/Databases

The INTERPOL DNA Gateway – Official Publication Février 2017

The INTERPOL Facial Images Best Practices Guide Octobre 2015 & Facial Recognition Fact Sheet

INTERPOL Guidelines concerning Fingerprint Transmission 2012

INTERPOL Rules on the processing of information for the purposes of international police co-operation

ETIAS
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

www.un.org/sc/ctc/

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20161116/factsheet_-_etias_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-3706_en.htm

NIST Special Publication 1152 'Latent Interoperability Transmission Specification' www.nist.gov

4. ANNEXES

4.1 Acronymes

CFA Contrôle des frontières automatisé

AFIS Automatic Fingerprint Identification System (Système d'identification automatique d'empreintes digitales)

RPCV Renseignements préalables concernant les voyageurs

PFF Point de franchissement des frontières

BMS Border Management Information System (Systèmes d'information de gestion des frontières)

CCF Commission de contrôle des fichiers d'INTERPOL

CCTV Closed Circuit Television (Vidéosurveillance)

eBMS Electronic Border Management Information System (Système électronique d'information de gestion des frontières)

TEE Taux d'erreur égale

ETS Electronic Travel Systems (Systèmes électroniques de voyage)

TAF Taux d'acceptation fausse

TRF Taux de rejet faux

TDA Taux de défaillance d'acquisition

CTE Combattants terroristes étrangers

IEC International Electrotechnical Commission (Commission électrotechnique internationale)

OACI Organisation de l'aviation civile internationale

RPCVi Renseignements préalables concernant les voyageurs interactifs

ISO International Organization for Standards (Organisation internationale de normalisation)

SDL Structure de données logique

ZLA Zone de lecture automatique

ICP Infrastructure à clés publiques

PNR Passenger Name Record (Données des dossiers passagers)

SMQ Système de management de la qualité

SIS Système d'information Schengen

STR Short Tandem Repeat (Séquence répétitive courte)

TAA Taux d'acceptation authentique

TRA Taux de rejet authentique

SIV Système européen d'identification des visas

4.2 Glossaire de termes et expressions en biométrie

Accréditation – L'ISO définit l'accréditation comme la « reconnaissance formelle par un organisme indépendant, en général un organisme d'accréditation, qu'un organisme de certification est compétent pour procéder à la certification ».

Système d'identification automatique d'empreintes digitales – Un système électronique conçu pour stocker et interroger de grands volumes (1) d'ensembles de référence d'empreintes digitales et palmaires et (2) de marques de doigt et de paume de scènes de crime. Les recherches de gestion de l'identité génèrent habituellement une seule réponse ou aucun résultat de trace. Les résultats d'une recherche de détection de crimes sont présentés sous forme de liste de réponses de correspondances possibles. Les réponses sont examinées par un expert en empreintes digitales qui confirme toute correspondance produite par le système.

Modalité biométrique – le type de données biométriques employées dans un système ou un contexte opérationnel, ainsi des empreintes digitales, visages, iris, etc.

Certification – l'ISO définit la certification comme une « assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques ».

Évaluation de la conformité – L'IEC définit l'évaluation de la conformité comme la « démonstration que des exigences spécifiées concernant un produit, un processus, une personne ou un organisme sont satisfaites ».

Recherche de détection de crimes – un protocole de recherche bidirectionnel interrogeant (1) des données de référence en fonction des données de scène de crime et (2) des données de scène de crime en fonction des données de référence.

Données de scène de crime – générées à partir d'échantillons et d'éléments prélevés sur les scènes de crime.

Taux d'erreur égale (TEE) se réfère au réglage de seuil spécifique pour lequel le Taux d'acceptation fausse et le Taux de rejet faux sont égaux.

Gestion des exceptions – mesures contingentes introduites en cas de défaillance d'un système biométrique, ainsi intervention humaine, systèmes de secours, etc.

Taux de défaillance d'acquisition (TDA) - la proportion de toutes les transactions enregistrées qui ne peuvent aboutir du fait de défaillances lors des phases de présentation (aucune image capturée), d'extraction de caractéristiques ou de contrôle qualité.

Taux d'acceptation fausse (TAF) – le nombre d'acceptations fausses en proportion du nombre total de requêtes biométriques qui auraient dû être rejetées, soit le nombre de défauts de correspondance *générés et présentés par le système* en proportion des défauts de correspondance véridiques

Taux de rejet faux (TRF) – le nombre de rejets faux en proportion du nombre total de requêtes biométriques qui auraient dû être acceptées, soit le nombre de correspondances *générées et présentées comme des défauts de correspondance par le système* en proportion des correspondances véridiques

Identification – (aussi dénommée comparaison 1 à plusieurs ou 1:n) Cette fonction de recherche ne dépend pas d'une identité suggérée. Elle interroge donc la base de données intégrale en quête d'une correspondance possible.

Recherche de gestion de l'identité – détermine si un sujet a déjà été inscrit dans une base de données en recherchant les données de référence biométriques du sujet dans les données de référence consignées dans le système.

Morphose – échantillons biométriques (ex. images faciales) de plusieurs donneurs fusionnés pour autoriser la vérification fructueuse de l'un quelconque des sujets donneurs par rapport à l'identité morphée.

Système de management de la qualité – Un protocole formel définissant et documentant les processus, procédures et responsabilités pour atteindre des objectifs de qualité. Le système est pensé pour coordonner et diriger les activités d'une organisation afin de respecter les exigences des clients et de la réglementation, de faire face aux défauts de conformité et d'engendrer une culture d'amélioration continue.

Données de référence – prélevées sous des conditions contrôlées sur des individus détenus ou soupçonnés d'un délit, ainsi les empreintes digitales des 10 doigts des mains capturées électroniquement avec un scanner ou par des méthodes traditionnelles avec de l'encre et du papier, les frottis buccaux prélevés à l'intérieur de la joue d'un prévenu ou un cheveux, voire un échantillon sanguin, traité afin de générer un profil ADN complet, des photographies numériques du visage, etc.

Recherche d'événements /délits en série – la recherche de données criminalistiques ou biométriques de scène de crime dans une base de données de données de scène de crime similaires pour identifier une quelconque correspondance et ainsi établir des liens entre les crimes ou entre les événements d'une enquête unique.

Usurpation – (aussi dénommée attaque de présentation) correspond à la présentation de fausses données biométriques (ainsi un masque facial en latex, une photographie, une fausse empreinte digitale ou vocale) d'un utilisateur inscrit légitime pour obtenir un accès sans autorisation à un système de reconnaissance biométrique

Seuil - Un réglage ajustable des systèmes biométriques. Il régule l'équilibre entre l'acceptation et le rejet pour une application donnée.

Rendement – Le volume de personnes utilisant un système biométrique durant une plage horaire définie.

Taux d'acceptation authentique (TAA) – La mesure de la capacité du système à faire correspondre correctement les attributs identitaires biométriques de la même personne.

Taux de rejet authentique (TRA) – La mesure du nombre d'occasions où les attributs identitaires biométriques d'une personne ne correspondent correctement *pas* aux attributs identitaires biométriques d'autres individus dans la base de données, soit la fréquence des défauts de correspondance corrects.

Vérification – (aussi dénommée comparaison un contre un ou 1:1). Ce modèle utilise une identité suggérée afin de sélectionner un seul modèle de la base de données pour le comparer avec le modèle

de requête. Il s'agit essentiellement d'un processus de comparaison du modèle de requête avec le modèle de la base de données pour confirmer, ou infirmer, que les deux modèles proviennent de la même personne.

4.3 Répertoire des organisations internationales

Biometrics Institute www.biometricsinstitute.org

Organisation de l'aviation civile internationale www.icao.int

Comité international de la Croix-Rouge www.icrc.org

Organisation internationale de police criminelle (INTERPOL) www.interpol.int

Commission électrotechnique internationale www.iec.ch

Organisation internationale de normalisation www.iso.org

4.4 Bureau de lutte contre le terrorisme (BLT) des Nations Unies

Le Secrétariat, les agences, les fonds et les programmes des Nations Unies ainsi que les organisations affiliées contribuent à la mise en œuvre de la Stratégie antiterroriste mondiale des Nations Unies grâce à leurs mandats individuels mais aussi leur appartenance à l'Équipe spéciale du Pacte mondial de coordination contre le terrorisme de l'Organisation des Nations Unies (GCTCCTF).

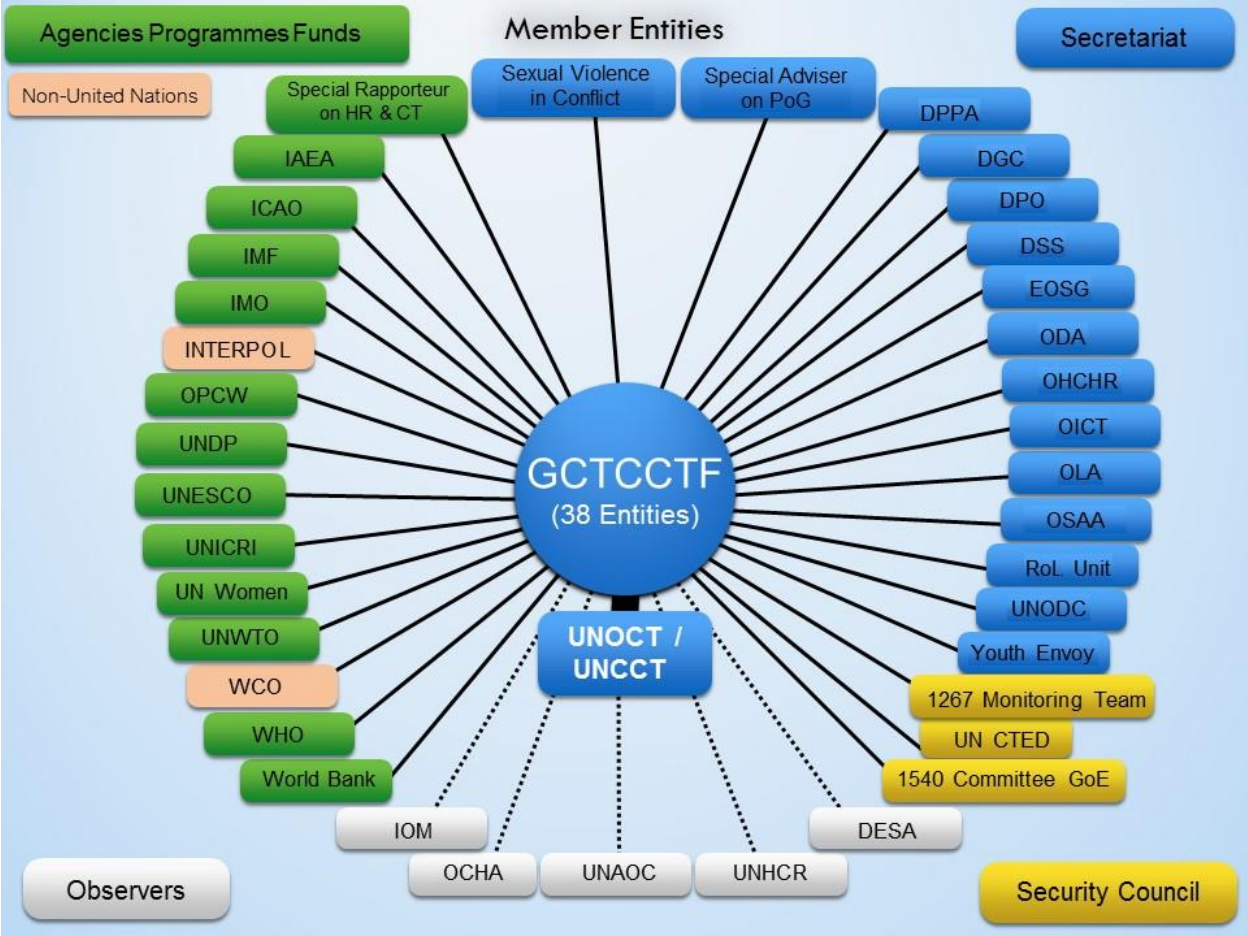
L'Équipe spéciale comprend 38 entités internationales et INTERPOL qui, de par leur travail, participent à l'effort multilatéral de lutte contre le terrorisme. Chaque entité apporte des contributions cohérentes avec son propre mandat. Les membres de l'Équipe spéciale incluent le BLT des NU et les entités suivantes :

1. Équipe de surveillance Al-Qaida/Taliban
2. Direction exécutive du Comité contre le terrorisme (DECT)
3. Département des opérations de paix (DPO)
4. Département des affaires politiques et de la consolidation de la paix (DPPA)
5. Département de la communication globale (DGC)
6. Département de la sûreté et de la sécurité (DSS)
7. Groupe d'experts du Comité 1540
8. Agence internationale de l'énergie atomique (AIEA)
9. Organisation de l'aviation civile internationale (OACI)
10. Organisation maritime internationale (OMI)
11. Fonds monétaire international (FMI)
12. Organisation internationale de police criminelle (INTERPOL)
13. Bureau des affaires de désarmement (ODA)
14. Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)
15. Bureau des affaires juridiques (OLA)
16. Bureau du Secrétaire général (OSG)

17. Bureau du Conseiller spécial pour la prévention du génocide
18. Bureau du Représentant spécial du Secrétaire général pour les enfants et les conflits armés (CAAC)
19. Bureau du Représentant spécial du Secrétaire général chargé de la question des violences sexuelles commises en période de conflit (SVC)
20. Bureau de l'Envoyé du Secrétaire général pour la jeunesse
21. Organisation pour l'interdiction des armes chimiques (OIAC)
22. Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste
23. Programme des Nations Unies pour le développement (PNUD)
24. Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO)
25. Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI)
26. Office des Nations Unies contre la drogue et le crime (ONUDC)
27. Bureau du Conseiller spécial pour l'Afrique des Nations Unies (OSAA)
28. Groupe de l'état de droit des Nations Unies
29. ONU-Femmes
30. Organisation mondiale du tourisme (OMT) des Nations Unies
31. Organisation mondiale des douanes (OMD)
32. Banque mondiale
33. Organisation mondiale de la Santé (OMS)

Observateurs

34. Organisation internationale pour les migrations (OIM)
35. Bureau de la coordination des affaires humanitaires (OCHA)
36. Département des affaires économiques et sociales des Nations Unies (DESA)
37. Haut-Commissariat des Nations Unies pour les réfugiés (UNHCR)
38. Alliance des civilisations de l'Organisation des Nations Unies (UNAOC)



4.5 Groupe de travail du BLT des Nations Unies sur la gestion des frontières et l'application de la loi dans le contexte de la lutte contre le terrorisme

Ce Groupe de travail interorganisations des Nations Unies a pour objet de guider les États membres dans le cadre de la mise en œuvre des mesures juridiques, institutionnelles et pratiques nécessaires pour la gestion des frontières dans le contexte de la lutte contre le terrorisme. Il privilégie en particulier les domaines suivants : mobilité des terroristes, intégrité et sécurité des documents de voyage, mouvements illicites d'espèces et d'instruments négociables au porteur, mouvement et traitement de marchandises, mouvements illicites des armes légères et de petit calibre, munitions, explosifs et armes de destruction massive, sécurité aérienne et maritime, systèmes d'alerte anticipée et d'alerte et contrôle des frontières ouvertes.

Mandat

Le Groupe de travail a été créé pour aider les États membres à renforcer la gestion de leurs systèmes de gestion des frontières et de contrôle des frontières comme énoncé dans le Pilier II, paragraphes 4, 5, 7, 8 et 13 à 16 et dans le Pilier III, paragraphes 2, 4 et 11 à 13 de la Stratégie antiterroriste mondiale des Nations Unies A/RES/60/288).

Mandat développé pour le Groupe de travail sur la gestion des frontières dans le contexte de la lutte contre le terrorisme.

Statut

Actuellement, le Groupe de travail met en œuvre un projet de coordination de la gestion des frontières, compilant toutes les conventions, normes et bonnes pratiques internationales pertinentes sous un format exploitable et convivial pour aider les États intéressés afin de construire des mécanismes institutionnels et procéduraux pour un système efficace de gestion des frontières. Le Groupe de travail a finalisé un modèle de travail sur la gestion des frontières coordonnée. Ce modèle doit continuer à être amélioré grâce à des consultations et à un dialogue permanents avec les États membres et les organisations internationales.

Entités

Co-présidents :

- Direction exécutive du Comité contre le terrorisme (DECT)(principal)
- Organisation mondiale des douanes (OMD)
- Organisation internationale de police criminelle (INTERPOL)

Entités de base :

- Bureau de lutte contre le terrorisme (BLT) des Nations Unies
- Équipe spéciale du Pacte mondial de coordination contre le terrorisme de l'Organisation des Nations Unies (GCTCCTF)
- Organisation de l'aviation civile internationale (OACI)
- Organisation maritime internationale (OMI)
- Office des Nations Unies contre la drogue et le crime (ONUDC)
- Organisation internationale pour les migrations (OIM)
- Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH)
- Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI)
- Bureau des affaires de désarmement (ODA)
- Équipe de surveillance 1267
- Groupe d'experts du Comité 1540
- Haut-Commissariat des Nations Unies pour les réfugiés (UNHCR) (Observateur)

Autres entités membres :

- Département des opérations de paix (DPO)
- Organisation pour l'interdiction des armes chimiques (OIAC)
- Programme des Nations Unies pour le développement (PNUD)
- Organisation mondiale de la Santé (OMS)
- Département des affaires économiques et sociales (DESA)

Le Groupe de travail déploie ses activités selon plusieurs thèmes clés :

- Mobilité et traitement des personnes
- Intégrité et sécurité du processus de délivrance de document
- Mouvement d'espèces et autres instruments négociables au porteur
- Mouvement et traitement des marchandises
- Mouvements des armes légères et de petit calibre, munitions, explosifs et CBRN
- Sécurité maritime
- Sécurité aérienne
- Systèmes d'alerte anticipée et d'alerte

- Contrôle des frontières ouvertes
- Besoin primordial de respect des droits de l'homme

Mobilité et traitement des personnes

L'une des conséquences significatives des attaques terroristes menées ces dernières années dans le monde entier porte sur la liaison croissante entre les mouvements transfrontaliers de personnes et les mesures de protection de la sécurité nationale. Comme les processus mêmes facilitant les voyages ainsi que les échanges économiques et culturels sont également exploités par les terroristes, les mesures de prévention du terrorisme sont devenues explicitement liées à la gestion et à la régulation des mouvements transfrontaliers. Ces mesures incluent la mise en œuvre de systèmes de gestion des frontières intégrés pour les passagers, la délivrance de documents de voyage sécurisés, la promotion des échanges d'informations entre les parties prenantes, la formation et le développement des capacités. Les améliorations dans ces domaines peuvent contribuer à rehausser la sécurité et les systèmes d'immigration tout en facilitant les mouvements transfrontaliers de personnes. Certaines de ces mesures sont complexes technologiquement et hautement innovantes mais nombre de mesures plus simples peuvent être mises en œuvre dans des secteurs traditionnels de la gestion des migrations afin de parachever les capacités d'ensemble. Ces mesures devraient systématiquement être justifiées par le niveau de menace existant, particulièrement car l'augmentation de la sécurité peut entraîner une progression des obstructions et une intrusion potentielle dans les droits civils et à la vie privée.

Intégrité et sécurité du processus de délivrance de document

La gestion de l'identité et de la sécurité des documents de voyage sont des outils importants de la prévention de la mobilité des terroristes et de la lutte contre la criminalité transfrontalière. Entre les mains des terroristes, un document de voyage frauduleux peut s'avérer aussi dangereux qu'une arme. Les passeports sont toujours plus sécurisés et difficiles à contrefaire. Criminels et terroristes redoublent donc d'efforts pour falsifier les documents justificatifs (certificats de naissance, cartes d'identité nationales, etc.) ou demander des passeports « délivrés officiellement ». Il s'avère donc essentiel que les États développent et mettent en œuvre des spécifications universelles de gestion de l'identité et de sécurité des documents de voyage (notamment durant le processus de délivrance) pour résoudre ces vulnérabilités.

Mouvement d'espèces et autres instruments négociables au porteur

La contrebande transfrontalière d'espèces ou d'instruments négociables au porteur (INP) figure parmi les méthodes de prédilection des terroristes afin de faire passer des frontières internationales à des fonds, aux fins de financement du terrorisme ou de blanchiment des produits d'activités illicites. Les gouvernements confient à leurs services des douanes la mise en œuvre des mesures de contrôle des frontières dans le respect des normes internationales afin de détecter et d'éviter les mouvements illicites d'espèces et d'INP. Une conformité rigoureuse avec ces normes améliorerait l'efficacité du contrôle des frontières dans ce domaine. La lutte contre le financement du terrorisme forme partie intégrante de l'approche de lutte contre le terrorisme des Nations Unies, reflétée par ses maintes résolutions et conventions.

Mouvement et traitement des marchandises

Le commerce global et la chaîne logistique internationale sont particulièrement vulnérables aux manipulations des terroristes. Afin de minimiser cette vulnérabilité, un éventail de mesures devraient être adoptées, notamment l'assurance de la réception des informations anticipées électroniques sur les marchandises des expéditions en entrée, en sortie et en transit, l'emploi d'une approche cohérente de gestion du risque pour faire face aux menaces sur la sécurité des marchandises, l'usage d'équipements de détection non intrusifs, la promotion de la coopération entre les administrations des douanes (ainsi l'exécution d'une inspection en sortie des marchandises et conteneurs à haut risque) et la création de partenariats avec le secteur privé pour la mise en œuvre de pratiques sécurisées à chaque stade de la chaîne logistique via les programmes d'Opérateur économique agréé (OEA). La mise en œuvre de ces mesures et d'autres connexes est essentielle pour accroître la sécurité du commerce international et faciliter les flux de marchandises aux frontières internationales.

Mouvements des armes légères et de petit calibre, munitions, explosifs et CBRN

Le trafic et les mouvements illicites des armes légères et de petit calibre, des munitions, des explosifs et des substances CBRN (chimiques, biologiques, radiologiques et nucléaires) ainsi que des biens à double usage, pondérés par les évolutions des pratiques du commerce des armes et l'implication d'acteurs étrangers au secteur, présentent des problèmes significatifs qui doivent être résolus par des efforts globaux de lutte contre le terrorisme. Aux mains des terroristes, ces munitions et ces substances deviennent les ingrédients des attaques terroristes. Une réglementation, des contrôles des exportations et une gestion des frontières efficaces, incluant des mesures législatives et de mise en exécution, peuvent minimiser les risques de détournement de ces éléments ou d'acquisition illicites par des acteurs non publics. Ces mesures devraient respecter le besoin de maintien d'un équilibre approprié entre les contrôles sur les exportations et la facilitation du commerce légitime.

Sécurité maritime

Plus de 90 pour cent de la totalité des biens négociés internationalement sont transportés de l'origine à la destination selon les principales voies maritimes globales dans le monde. La sécurité du domaine maritime est donc une question d'importance globale. La sécurité maritime a pour objet de détecter et de dissuader les menaces contre la sécurité, de prendre des mesures préventives contre les incidents de sécurité affectant les navires ou les installations portuaires et de protéger les passagers, équipages, navires et chargements, installations portuaires et personnes travaillant et vivant dans les zones portuaires tout en assurant le flux efficient en toute sécurité du commerce maritime. La mise en œuvre efficace de la législation et des mesures de sécurité pratiques pertinentes est nécessaire afin d'éviter des actes illégaux à l'encontre des passagers et de l'équipage des navires dans le cadre des voyages internationaux et des installations portuaires qui les servent.

Sécurité aérienne

Les actes de terrorisme demeurent des menaces graves et constantes pour l'aviation civile internationale. La confrontation avec ces menaces exige la création de mesures de sécurité et de politiques responsables et exhaustives destinées à assurer la sécurité physique des aéronefs et aéroports. L'adoption de dispositions législatives de criminalisation des actes d'interférence illégale

à l'encontre de l'aviation civile et la mise en œuvre et en exécution efficace des normes et pratiques de sécurité aérienne pertinentes rehausseraient significativement la capacité des États à se défendre de ces menaces.

Systèmes d'alerte anticipée et d'alerte

La sécurité aux frontières est un processus dynamique et évolutif. Comme les mouvements transfrontaliers illégaux de personnes compromettent non seulement la sécurité mais aussi le bien-être politique, économique et social des États, les gouvernements priorisent désormais les efforts de coopération en matière de sécurité, conscients que les actions unilatérales ne sont aujourd'hui plus efficaces. Des systèmes complets d'alerte anticipée et d'alerte sont donc des composants clés des systèmes efficaces de gestion des frontières. Ils renforcent la capacité collective des États de détection, de prévention et de lutte contre le terrorisme en facilitant la coopération entre les organismes ainsi que le partage et l'échange en temps opportun d'informations fiables et pertinentes pour assurer la prise de décisions critiques de manière responsable.

Maintes organisations internationales dotées d'un mandat de contrôle des frontières emploient ou promeuvent les systèmes d'alerte anticipée et d'alerte, que ce soit à l'aide d'outils développés par chaque organisation individuelle ou destinés à être exploités par la communauté internationale. Ces outils incluent les réseaux CEN et RILO de l'OMD, les réseaux SOLAS, LRIT et AIS de l'OMI, les Listes consolidées des comités de sanctions du Conseil de sécurité ainsi que le système de communications global sécurisé I-24/7, la base de données SLTD et le régime des Notices de l'Organisation internationale de police criminelle (INTERPOL).

Contrôle des frontières ouvertes

Une frontière ouverte (celle entre la frontière terrestre officielle et les points de contrôle des ports maritimes) facilite les mouvements transfrontaliers illégaux de personnes, notamment les terroristes et les criminels, et de marchandises (notamment les armes légères et de petit calibre, munitions, explosifs et substances chimiques, biologiques, radiologiques et nucléaires). Les gouvernements reconnaissent l'importance de la sécurisation d'une frontière ouverte et s'efforcent d'y procéder avec une diversité de mesures incluant la surveillance, les patrouilles, les barrières physiques, les opérations et patrouilles sous commandement commun, les échanges d'informations, les appréciations de renseignements et l'engagement au sein des communautés frontalières sur les questions de contrôle et de police. Des efforts de contrôle concertés des autorités concernées sont nécessaires pour faire face efficacement aux risques présentés par les frontières ouvertes.

Besoin primordial de respect des droits de l'homme

La Stratégie antiterroriste mondiale des Nations Unies reflète une affirmation claire de la part des États membres : des mesures efficaces de lutte contre le terrorisme et la protection des droits de l'homme ne sont pas des buts en conflit mais plutôt complémentaires en se renforçant mutuellement. Les droits de l'homme et la règle de l'état de droit constituent les fondamentaux de l'effort global de lutte contre le terrorisme. En adoptant la Stratégie mondiale et son Plan d'action, les États membres ont décidé « De reconnaître que la coopération internationale et toutes les mesures que nous prenons pour prévenir et combattre le terrorisme doivent être conformes aux obligations que nous impose le droit international, notamment la Charte des Nations Unies et les conventions et protocoles

internationaux pertinents, en particulier les instruments relatifs aux droits de l'homme, le droit des réfugiés et le droit international humanitaire » (A/RES/60/288, Annexe, préambule paragraphe 3, réaffirmé dans A/RES/64/297). L'Assemblée Générale a aussi souligné le besoin primordial d'assurer le respect des droits de l'homme dans le cadre des efforts de lutte contre le terrorisme dans plus de 60 résolutions concernant le terrorisme international. Plus spécifiquement pour le contrôle des frontières, l'Assemblée a demandé aux États « de veiller à ce que les directives et les pratiques mises en œuvre dans toutes les opérations de contrôle aux frontières ou dans tout autre mécanisme de préadmission soient clairement définies et respectent intégralement les obligations que leur impose le droit international, en particulier des réfugiés et des droits de l'homme, à l'égard des personnes se réclamant de la protection internationale » (A/RES/62/159, paragraphe 8, réaffirmé par A/RES/64/221).