Centre pour la quatrième
révolution industrielle

WORLD ECONOMIC FORUM

Cadre d'action pour un usage responsable de la reconnaissance faciale

Cas d'usage : gestion des flux

Partie II
Projet pilote : Auto-évaluation, audit des systèmes de gestion et certification

LIVRE BLANC

DECEMBRE 2020

Couverture: Getty Images/da-kuk

Intérieur: Getty Images/Prostock-Studio; Getty Images/Izisek; Getty Images/KENGKAT; Getty Images/Wonry; Getty Images/DNY59; Getty Images/Imaginima; Getty Images/MangoStar_Studio

Table des matières

Avant-propos

La première initiative mondiale pour renforcer la confiance et la transparence dans l'utilisation de la reconnaissance faciale

Kay Firth-Butterfield,
Responsable de l'intelligence artificielle et de l'apprentissage machine ; membre du comité exécutif du Forum Économique Mondial

Hideharu Miyamoto,
Senior Executive Officer, Aéroport international de Narita, Japon

Julien Nizri,
Directeur général,
AFNOR Certification, France

Toshifumi Yoshizaki,
Vice-président senior,
NEC Corporation,
JaponPréface

Il n'a jamais été aussi crucial de disposer d'une technologie sans contact permettant d'identifier avec précision différents publics : les clients, les employés et les fournisseurs. Dans cette optique, le Forum Économique Mondial a lancé l'année dernière une initiative visant à mettre en place un cadre de gouvernance pour l'usage responsable de la technologie de reconnaissance faciale et de la biométrie à distance dans le contexte d'une meilleure expérience d'embarquement des passagers de compagnies aériennes. Si l'an dernier, disposer de ces technologies était un simple avantage, aujourd'hui, en pleine pandémie mondiale de COVID-19, la biométrie à distance est devenue indispensable.

Bien que l'industrie aéroportuaire utilise les technologies numériques depuis des décennies, l'intelligence artificielle vient fondamentalement transformer l'expérience des passagers, en réduisant les temps d'attente et renforçant le confort d'utilisation. Mais ce progrès n'est pas sans compromis ni risques. La reconnaissance faciale soulève des craintes légitimes liées aux risques de biais, de discrimination potentielle et d'exposition aux données personnelles. Afin de traiter ces questions de manière proactive, nous avons combiné nos efforts pour élaborer une définition globale de ce que représente l'usage responsable de la reconnaissance faciale pour les cas d'usage de la gestion des flux et un cadre de gouvernance pour rendre cette définition opérationnelle.

Suivant la méthodologie proposée dans ce Livre blanc et dans un souci de transparence, l'aéroport international de Tokyo-Narita et NEC Corporation ont rejoint l'initiative du Forum pour tester le questionnaire d'évaluation présenté dans le premier Livre blanc de ce projet pilote, intitulé « Cadre d'action pour un usage responsable de la reconnaissance faciale - Cas d'usage : gestion des flux ». Ils ont suivi une approche pionnière et décidé de partager publiquement leurs résultats afin de démontrer aux acteurs du secteur et aux décideurs politiques comment allier transparence et confiance des passagers.

Ce Livre blanc vise à faire avancer la discussion sur la certification et les audits par des tiers pour le déploiement responsable de la technologie de reconnaissance faciale. À cet égard, AFNOR Certification a joué un rôle essentiel en concevant un référentiel d'audit pour la phase pilote de cette initiative, qui est maintenant prêt à être testé par des organismes volontaires pour valider le système de certification tierce-partie.

Le Forum Économique Mondial encourage les organisations à rejoindre cette initiative pour tester et adopter ce cadre et s'engager globalement dans l'utilisation responsable des systèmes de reconnaissance faciale.

Preface

“ Le groupe de travail a été initialement composé de représentants de l’industrie envisageant de se procurer des systèmes de reconnaissance faciale.

En avril 2019, le Centre pour la quatrième révolution industrielle du Forum Économique Mondial a lancé le projet sur l’usage responsable de la reconnaissance faciale. Il tend à répondre au besoin de lignes directrices concrètes pour garantir une utilisation fiable et sûre de cette technologie à travers la conception d’un cadre de gouvernance solide. Pour atteindre cet objectif, le Forum a bâti un projet de gouvernance multipartite basé sur une expérimentation, avec la France, et le Japon qui a récemment rejoint l’initiative, en tant que partenaires principaux. Le groupe de travail a été initialement composé de représentants de l’industrie envisageant de se procurer des systèmes de reconnaissance faciale (Groupe ADP et SNCF), de fournisseurs de technologies (Amazon Web Services, IDEMIA, IN Groupe et Microsoft), de décideurs politiques (membres du Parlement français), d’universitaires, d’organisations de la société civile et d’AFNOR Certification.

Pendant la phase de conception, ce groupe de travail a décidé d’adopter une approche par cas d’usage, car les risques associés aux systèmes de reconnaissance faciale dépendent largement du contexte dans lequel la technologie est déployée. En effet, des faux positifs et des faux négatifs peuvent conduire à des résultats très différents si un système donné est utilisé pour accélérer un processus d’embarquement ou pour pister un suspect. Par conséquent, en se concentrant sur une application concrète, un système spécifique et les parties prenantes potentiellement concernés par ce système (par exemple, les passagers des compagnies aériennes), la possibilité de concevoir conjointement un cadre de gouvernance qui atténue efficacement les risques associés est plus sure.

Après mûre réflexion, les membres du groupe de travail ont décidé de se concentrer sur la « gestion des flux » (utilisation des traits du visage comme moyen d’accès à un service) principalement parce que ce cas d’usage est susceptible de se développer dans les années à venir. Par exemple, les organisateurs des Jeux olympiques de Tokyo ont annoncé l’usage de la reconnaissance faciale pour gérer l’accès des athlètes et du personnel dans les stades et dans les installations olympiques.[1] Les aéroports et les compagnies aériennes ont également commencé à utiliser cette technologie.[2]

Afin de concevoir un cadre de gouvernance équilibré et exploitable, le groupe de travail a élaboré une méthode structurée en quatre étapes : 1) définir ce qui constitue un usage responsable de la technologie de reconnaissance faciale (TRF) en rédigeant un ensemble de principes d’action ; 2) concevoir un ensemble de bonnes pratiques pour faciliter l’application de ces principes ; 3) s’assurer au moyen d’un questionnaire d’évaluation que les organisations s’y conforment ; et 4) valider le respect des principes d’action au moyen d’un référentiel d’audit et d’un système de certification.

Pour ce dernier point, un partenariat a été signé avec AFNOR Certification, dont l’expertise en matière d’audit et de certification est reconnue au niveau international. Considérant que l’objectif principal de cette initiative permet d’atténuer les risques pouvant entraîner une altération ou une interruption du service offert aux passagers lorsque les aéroports déploient des systèmes de reconnaissance faciale, AFNOR Certification a suggéré de concevoir un audit de l’organisation humaine et de la rigueur des procédés, plutôt qu’un audit des algorithmes de reconnaissance faciale, pour deux raisons principales. Premièrement, les compagnies aéroportuaires sont responsables de la qualité du service qu’elles fournissent à leurs clients et ont besoin de conseils sur la manière d’améliorer l’organisation qui permet d’assurer cette qualité. Elles seront soutenues dans ce processus, en s’appuyant sur des bases solides qui respectent les normes de management de de la qualité ISO 9000. Deuxièmement, bien que cette étape soit cruciale, auditer directement des algorithmes de reconnaissance faciale soulève un ensemble de défis fondamentaux pour un organisme de certification. Par exemple, quel est le seuil de performance acceptable pour les systèmes en fonctionnement, surtout lorsque cette performance est dynamique et en constante évolution ? Comment traduire les considérations juridiques et éthiques (par exemple l’équité) en exigences quantitatives pouvant être évaluées ? Comment remédier au manque de transparence des systèmes d’IA et produire des décisions pouvant être interprétées ? Ces questions complexes et ouvertes nécessitent des recherches plus approfondies. Réaliser un audit de l’organisation humaine et de la rigueur des procédés permet d’assurer un premier niveau de garantie de l’usage responsable de la TRF pour la gestion des flux.

Intéressées par cette approche pratique, les parties prenantes japonaises cherchant à poursuivre leurs efforts pour garantir l’usage responsable de la TRF dans les aéroports ont décidé de se joindre à notre initiative. À cette fin, le gouvernement japonais et NEC Corporation ont nommé deux experts pour travailler au Centre pour la quatrième révolution industrielle du Forum Économique Mondial au Japon, où ils jouent un rôle essentiel dans l’élaboration de cette initiative. Le gouvernement du Japon et NEC sont des partenaires très précieux pour deux raisons principales. Tout d’abord, la TRF est déployée dans les aéroports japonais et offre ainsi un cas d’usage pertinent. En effet, l’année dernière, l’aéroport international de Narita - premier aéroport du Japon, avec plus de 41 millions de passagers par an[3] - a annoncé son intention de commencer à déployer cette technologie en 2020 pour améliorer les contrôles de sécurité et le processus d’embarquement grâce au service One ID[4] fourni par NEC. Plus récemment, le

gouvernement japonais a publié des lignes directrices sur la protection des données biométriques afin de réglementer cette utilisation.[5] Deuxièmement, l'aéroport international de Narita a accepté d'auto-évaluer son système de reconnaissance faciale en utilisant le questionnaire d'évaluation présenté dans le premier Livre blanc.[6] Cette collaboration représente donc une opportunité pour l'aéroport de promouvoir la transparence et la responsabilité pour ses passagers locaux et mondiaux.

Les trois premières étapes de cette méthode ont été présentées en détail, dans le premier Livre blanc, publié en février 2020. Dans le présent document, qui constitue la deuxième partie, l'accent est mis sur la dernière étape - l'introduction du référentiel d'audit et du système de certification conçus conjointement pour les acteurs de l'industrie. Les réponses de l'aéroport international de Narita au questionnaire d'évaluation sont également présentées comme un exemple d'auto-évaluation rigoureuse.

Introduction

La nécessité d’un cadre de gouvernance équilibré pour la technologie de reconnaissance faciale n’a jamais été aussi critique.

« L'objectif principal de cette initiative du Forum Économique Mondial est d'établir un cadre de gouvernance global pour garantir l'usage responsable de la TRF.

Au cours des dernières années, les progrès technologiques rapides, dus principalement aux progrès de l'apprentissage machine et des capteurs, ont contribué au développement de la TRF. Cela a permis son déploiement commercial, au-delà des laboratoires scientifiques où elle était jusque-là contenue. En effet, cette technologie s'est maintenant étendue à divers domaines de la vie publique et privée, y compris dans les banques, le commerce de détail, les transports, le maintien de l'ordre et même les soins de santé.

Le développement de la TRF crée de considérables opportunités d'utilisations, bénéfiques d'un point de vue social, principalement grâce à l'amélioration des processus d'authentification et d'identification, qu'il s'agisse de déverrouiller un téléphone, monter à bord d'un avion et accéder aux services publics en ligne. Mais elle peut également porter atteinte aux libertés civiles ou produire des effets discriminants. Par exemple, aux États-Unis, des lieux de divertissement[7] ont utilisé cette technologie sur des consommateurs sans préavis ni consentement. Des atteintes à l'intégrité des données[8] liées à la biométrie à distance sont régulièrement signalées et des solutions puissantes de reconnaissance faciale sont mises en place grâce à des pratiques controversées de scraping de données (une technique d'extraction).[9] Récemment, cette technologie a conduit à l'arrestation et à la détention injustifiées d'un Afro-Américain innocent[10]

Ces controverses ont conduit à une intensification du débat politique. Aux États-Unis, plusieurs villes ont interdit l'utilisation de la TRF par les agences municipales, y compris en Californie (San Francisco,[11] Oakland[12]) et cinq villes du Massachusetts (Boston,[13] Brookline,[14] Cambridge,[15] Northampton[16] et Somerville[17]), tandis que Portland, dans l'Oregon, a interdit l'utilisation publique et privée de cette technologie dans les espaces publics.[18] À l'échelle des États, Washington a été le premier État à adopter une loi[19] visant à mettre en place des garde-fous liés à l'utilisation de la TRF par le gouvernement. Des législateurs démocrates ont proposé une législation fédérale[20] pour interdire définitivement son utilisation par les forces de l'ordre. Cette initiative vient compléter la liste des propositions politiques en cours de discussion entre les différentes parties prenantes, qui comprend différents ensembles de principes,[21] un moratoire[22] et la création d'un nouveau bureau fédéral[23] : un régulateur dédié à la TRF.

En outre, de grandes entreprises technologiques ont également exprimé leur opinion sur ce sujet. Ainsi, Microsoft[24] s'est engagé à ne plus vendre de TRF aux forces de l'ordre tant qu'une réglementation fédérale n'aura pas été mise en place. Amazon Web Services (AWS)[25] a mis en place un moratoire d'un an sur l'utilisation par la police de sa plateforme Rekognition, tandis qu'IBM a annoncé qu'il ne proposera, ne développera et ne fera plus de recherche sur la TRF.[26]

Un Livre blanc de la Commission européenne publié en février 2020 sur la gouvernance de l'intelligence artificielle[27] examine attentivement la possibilité d'introduire des exigences supplémentaires pour limiter le déploiement de la TRF. En janvier, dans la version préliminaire du document, la Commission européenne aurait envisagé d'introduire un moratoire de cinq ans[28] sur l'usage de la reconnaissance faciale dans les espaces publics afin d'accorder du temps pour élaborer une réglementation appropriée, mais n'a pas mentionné cette option dans la version publiée.

Il n'est pas surprenant que la plupart de ces prises de positions politiques soient liées à l'utilisation de cette technologie par le gouvernement et les forces de l'ordre, car dans ces domaines, le risque d'abus et la surveillance de populations fragiles sont élevés. Il est certain que, compte tenu de la sensibilité des données biométriques, l'utilisation de la reconnaissance faciale est risquée par nature. En effet, monter à bord d'un avion dont la compagnie utilise la reconnaissance faciale, accéder à un stade, ou utiliser la publicité basée sur l'analyse des visages dans le commerce de détail comportent également des risques comme par exemple : la violation de la vie privée, les inégalités d'accès aux services en raison des écarts de performances entre les différentes catégories démographiques, etc. Il est donc nécessaire d'identifier et d'atténuer efficacement les risques dans tous les cas d'usage. L'objectif principal de cette initiative du Forum Économique Mondial est d'établir un cadre de gouvernance global pour garantir l'usage responsable de la TRF, en commençant par le cas d'usage de la gestion des flux.

Le Livre blanc publié précédemment, « Cadre d'action pour un usage responsable de la reconnaissance faciale - Cas d'usage : gestion des flux » comportait deux sections principales : une présentation de notre méthodologie et son application au cas d'usage de la gestion des flux par le biais d'une méthode structurée en quatre étapes. Le présent Livre blanc est structuré en quatre sections. Tout d'abord, la présentation du cas d'usage de l'aéroport international de Narita, détaillant le test du questionnaire d'évaluation de l'aéroport effectué en collaboration avec NEC. Les réponses complètes figurent à l'annexe A. Ensuite, la présentation du référentiel d'audit, conçu conjointement avec AFNOR Certification, détaillant sa fonction, son ambition, ses différents usages et sa structure. Le référentiel complet est disponible à l'annexe B. Troisièmement, la description du système de certification, expliquant son objectif, ses avantages et son processus. Enfin, la présentation du parcours étape par étape, des principes à la délivrance du certificat, qu'un acteur de l'industrie doit accomplir pour démontrer son utilisation responsable de la TRF pour les applications de gestion des flux. Dans la dernière section, chaque étape présente les activités à mener.

Les deux Livres blancs combinés ont pour objectif d'aider les organisations à progresser vers un usage responsable de la TRF. Ils présentent la documentation que les organisations doivent prendre en compte (principes d'action, bonnes pratiques, questionnaire d'évaluation et référentiel d'audit) et la démarche qu'elles doivent suivre pour être certifiées.

Ces documents servent également un objectif plus vaste : faire avancer le débat sur la réglementation de la TRF aux niveaux local, régional et international en fournissant une méthode pratique d'atténuation des risques applicable à divers cas d'usage. Cette discussion et le projet pilote étant toujours en cours, le Forum Économique Mondial encourage les organisations impliquées ou désireuses de prendre part à la discussion à rejoindre cette initiative.

Methodologie

Une approche pilote réplicable dans d'autres cas d'utilisation de TRF

Une approche en quatre étapes

Le premier Livre blanc « Cadre d'action pour un usage responsable de la reconnaissance faciale - Cas d'usage : gestion des flux » a introduit une méthode basée sur quatre étapes principales (figure 1) pour construire un cadre de gouvernance solide capable de garantir l'usage responsable de la reconnaissance faciale :

1. **Définir** ce qui constitue un usage responsable des technologies de reconnaissance faciale en élaborant un ensemble de principes d'action. Le premier objectif du groupe de travail, composé de personnalités publiques, d'entreprises qui conçoivent et achètent des systèmes de reconnaissance faciale, d'organismes de réglementation, d'universitaires et de représentants de la société civile, était d'établir une définition commune, organisée autour de 11 principes
2. Concevoir un ensemble de méthodologies, adaptées aux cas d'usage, pour aider les équipes Produit dans le développement de leurs systèmes « responsables par design »
3. S'assurer du caractère responsable des systèmes développés à travers un questionnaire d'évaluation décrivant pour chaque cas d'usage les règles devant être respectées afin de répondre aux attentes des principes d'action
4. Valider le respect des principes d'action à travers la conception d'un référentiel d'audit par un tiers de confiance.

Chacune de ces étapes représente un niveau supplémentaire d'engagement de la part des acteurs de l'industrie en faveur d'un usage fiable de la TRF.

FIGURE 1:

Les quatre étapes pour assurer une conception et un usage responsables de la technologie de reconnaissance faciale pour les cas d'usage de la gestion des flux

Source : Forum Économique Mondial, "Cadre d'action pour un usage responsable de la reconnaissance faciale - Cas d'usage : gestion des flux", Livre blanc, février 2020

Testé dans le cadre d'un projet pilote avant déploiement

Conformément à l'approche expérimentale, chaque élément de ce cadre de gouvernance (principes d'action, bonnes pratiques, questionnaire d'évaluation et référentiel d'audit) sera testé et examiné sur la base des résultats pratiques du projet pilote. Si les résultats sont satisfaisants, le système de certification sera déployé en collaboration avec des organismes de certification partenaires, à commencer par AFNOR Certification, qui a joué un rôle clé dans cette initiative.

Une méthode évolutive et pouvant être reproduite

La méthodologie en quatre étapes pourrait être reproduite dans d'autres cas d'usage de la reconnaissance faciale. En effet, toute stratégie de déploiement responsable devrait commencer par établir une définition claire de ce qui constitue un usage responsable dans un domaine donné. Cela pourrait être réalisé en élaborant un ensemble de principes d'action à travers une approche multipartite. La définition peut ensuite être mise en œuvre lors du développement du produit, en fonction des exigences de conception appropriées ou des bonnes pratiques. Enfin, elle peut être testée au moyen d'un questionnaire d'évaluation puis validé par un référentiel d'audit. Par conséquent, les parties prenantes intéressées devront surtout déterminer quels éléments sont nécessaires pour adapter ces outils à leur contexte et à leur domaine d'activité.

1 Test du questionnaire d’évaluation par l’aéroport international de Narita

La première auto-évaluation publique de la reconnaissance faciale par une organisation

1.1 Cadre général et objectif

Le questionnaire d'évaluation sert de document d'auto-évaluation détaillant les exigences auxquelles doivent se conformer les organisations pour assurer le respect des principes d'action. En tant que tel, le questionnaire peut être utilisé individuellement pour effectuer une évaluation interne des processus existants, comme l'aéroport international de Narita a choisi de le faire (voir ci-dessous), ou en tant qu'outil pour mesurer la préparation au processus de certification (voir section 4).

Pour élaborer le questionnaire d'évaluation, chaque principe d'action a été divisé en une série de questions spécifiques à traiter par un groupe de travail interservices nommé par la direction. À cet égard, il est similaire au référentiel d'audit mais est moins détaillé.

1.2 Étude de cas : Le programme One ID à l'aéroport international de Narita, au Japon

Présentation de l'étude de cas

Le programme One ID accélérera le parcours des passagers depuis l'enregistrement, en passant par le dépôt des bagages, le contrôle de sécurité, et jusqu'à la porte d'embarquement

Source : Fourni par NEC Corporation

L'aéroport international de Narita, l'une des principales entreprises aéroportuaires du monde, a pour objectif d'offrir la meilleure expérience possible aux passagers, ce qui est particulièrement important car le Japon est l'une des destinations de voyage les plus populaires au monde.
Pour atteindre cet objectif, l'aéroport a décidé d'introduire le programme One ID utilisant la TRF pour accélérer le parcours passager, processus de l'enregistrement jusqu'à l'embarquement. Le projet a démarré en 2016 avec un objectif clair : permettre aux passagers de compléter leur parcours en limitant au maximum les arrêts

Ce système a été conçu pour fonctionner grâce aux données faciales des passagers enregistrées aux points de contact initiaux, comme les bornes en libre-service. Ces données sont liées à leurs passeports, qui contiennent des données électroniques et des informations sur la carte d'embarquement. Une fois le processus terminé, les voyageurs peuvent passer par l'ensemble des étapes de l'enregistrement jusqu'à l'embarquement sans présenter leur passeport ou leur carte d'embarquement. Ils pourront passer les contrôles de sécurité à l'entrée et les procédures d'embarquement à une cadence de marche normale. Ce processus fluidifié fait gagner beaucoup de temps aux passagers. Il représente également un outil précieux pour prévenir la propagation des maladies, en diminuant le risque de propagation de virus aux effets désastreux tels que ceux générés dans le monde entier par la pandémie de COVID-19.

La section suivante présente le programme One ID pour les acteurs de l'industrie potentiellement intéressés par le déploiement de solutions similaires.

Dimensions clés du système de reconnaissance faciale déployé

Expérience utilisateur
Il faut généralement environ 15 minutes à une compagnie aérienne pour compléter la procédure d'embarquement de tous les passagers à la porte d'embarquement. Pour atteindre cet objectif, l'expérience a été conçue de manière à permettre l'embarquement de 250 passagers répartis sur trois voies en 15 minutes. Lorsque l'aéroport international de Narita a mis en œuvre les exigences du système, il a suivi les directives de l'Agence des services d'immigration du Ministère de la Justice[29] et a pris en considération les résultats de l'évaluation[30] par le National Institute of Standards and Technology (NIST)[31] des algorithmes de reconnaissance faciale automatique pour atteindre le plus haut niveau de performance.

Une approche holistique était nécessaire pour réussir la mise en œuvre du système de reconnaissance faciale afin de garantir que les passagers passent par le processus d'enregistrement et d'embarquement à une cadence de marche normale. Prendre en compte les capacités de traitement du système de reconnaissance faciale n'était pas suffisant. Il a donc été décidé que NEC, le fournisseur de la solution technologique, en collaboration avec d'autres fournisseurs, testerait la disponibilité, la fiabilité et les performances du système à chaque point de contact (lors de l'enregistrement, du dépôt des bagages, du contrôle de sécurité et de l'embarquement).

Atténuation des biais
Conscient des problèmes de biais liés à la TRF, l'aéroport international de Narita a pris des mesures claires pour atténuer leurs effets négatifs potentiels, y compris en choisissant le fournisseur de technologie NEC Corporation, un leader mondial dans ce domaine. En effet, le NIST a mené en 2019 une solide étude[32] sur les effets de l'ethnie, de l'âge et du sexe sur le logiciel de reconnaissance faciale, en utilisant quatre grands ensembles de données. Il a évalué 189 algorithmes logiciels, en utilisant des ensembles de données du gouvernement fédéral contenant environ 18 millions d'images de 8,49 millions de personnes. L'étude a révélé des biais importants dans les logiciels de reconnaissance faciale relatifs aux personnes de couleur et aux femmes. La solution proposée par NEC s'est avérée être parmi les moins biaisées en termes d'âge, de sexe et d'ethnicité, tout en atteignant un niveau de précision élevé.[33] En outre, l'aéroport international de Narita s'est engagé à se conformer au plan de base de conception universelle[34] du Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme (MLIT) et aux lignes directrices en matière d'accessibilité de Tokyo 2020[35] pour les Jeux olympiques et paralympiques de Tokyo, qui visent tous deux à créer une société plus inclusive pour les personnes handicapées.

En outre, NEC avait pour mission principale de concevoir le logiciel de reconnaissance faciale, d'effectuer des tests de vérification et d'ajuster ses paramètres. Il a également travaillé en collaboration avec les compagnies aériennes sur l'installation des dispositifs, l'environnement lumineux, les tests opérationnels et les scénarios de formation pour assurer le meilleur déploiement possible.

Protection des données
La reconnaissance faciale est l'une des technologies biométriques les plus sensibles qui existent. En tant que tel, son déploiement nécessite beaucoup de soin et de considération quant à son impact potentiel sur la vie privée des 40 millions de passagers qui transitent chaque année par l'aéroport international de Narita. Le gouvernement japonais est pleinement conscient de ce défi. Pour assurer le déploiement responsable de la reconnaissance faciale dans les aéroports, le MLIT a nommé un groupe d'étude sur la gestion des données personnelles, un groupe de travail multipartite comprenant des représentants de l'Association internationale du transport aérien (IATA), de la Commission de protection des données personnelles, des experts juridiques et des associations de consommateurs. Pendant un an, le groupe de travail a mené une étude, qui a abouti à la publication de lignes directrices pour la gestion des données personnelles collectées par le programme One ID dans les aéroports.[36] Ce document comprend une liste des processus que les aéroports devraient suivre pour faire face aux risques de violation de la vie privée liés à ce service et garantir un niveau élevé de protection des données.

L'aéroport international de Narita applique strictement toutes les directives pour assurer le déploiement responsable du programme One ID. Il a accordé une attention particulière aux processus liés aux risques majeurs, tels que les violations de données biométriques. En effet, les cyberattaques étant plus sophistiquées de jour en jour, il est devenu de plus en plus difficile de les prévenir, tant pour les gouvernements que les grands groupes internationaux. Pour atténuer ce risque, les membres du groupe d'étude sur la gestion des données personnelles recommandent de supprimer dans les 24 heures les données biométriques recueillies lors des enregistrements. En outre, l'aéroport international de Narita effectue régulièrement des cyber-tests pour évaluer la robustesse de ses serveurs.

Réflexion sur la phase d'auto-évaluation
La volonté de l'aéroport international de Narita d'assurer l'usage responsable de la TRF pour la gestion des flux a pris forme lorsqu'il a envisagé de déployer cette technologie en 2016. À l'époque, il n'existait aucune directive officielle expliquant les processus à mettre en œuvre pour atteindre cet objectif. C'est pourquoi, dans un premier temps, l'aéroport a mené une réflexion interne, mais il est ravi de constater les progrès réalisés dans ce domaine au cours des quatre dernières années, d'abord au Japon et actuellement au niveau international grâce à l'initiative du Forum Économique Mondial.

Le processus multipartite lancé par le MLIT par l'intermédiaire du groupe d'étude sur la gestion des données personnelles et la publication des lignes directrices s'est avéré utile. Il a également aidé à préparer la phase d'auto-évaluation car de nombreux points énumérés dans le questionnaire, tels que ceux relatifs au droit à l'information et au consentement, avaient déjà été abordés dans les lignes directrices. La grande expérience du Japon sur ce sujet a été confirmée, et lorsque les réponses au questionnaire ont été examinées (voir l'annexe A), des progrès supplémentaires ont été observés, ce qui permet d'espérer atteindre un niveau de confiance supplémentaire de la part des passagers locaux et mondiaux grâce à cette initiative.

Toutefois, atteindre cette étape a demandé du temps. Alors que l'aéroport international de Narita a rejoint l'initiative du Forum sur l'usage responsable de la reconnaissance faciale début février 2020, le processus d'auto-évaluation n'a commencé que début mai et a duré six semaines, un délai supérieur à la projection initiale. Deux problèmes ont causé ce retard. Premièrement, le questionnaire d'évaluation est complet et couvre tous les aspects de la gestion du système : la gouvernance des données (par exemple, la sécurité et le caractère utilisable des données), la performance et la précision, et l'expérience utilisateur (UX). Par conséquent, pour répondre à toutes les questions, il a fallu faire appel à différents services au sein de l'aéroport international de Narita et de NEC Corporation. Deuxièmement, la déclaration de l'état d'urgence par le gouvernement japonais en réponse à la pandémie de COVID-19 a bouleversé le calendrier initial.

L'aéroport international de Narita espère que sa contribution aidera à améliorer le questionnaire d'évaluation comme le prévoit le processus itératif adopté par la communauté de projet. Par exemple, il recommande de renforcer la section relative à la sécurité des données et d'encourager les acteurs de l'industrie à suivre son approche consistant à supprimer les données biométriques dans les 24 heures suivant l'enregistrement des passagers. Il suggère également qu'il est moins nécessaire de procéder à un audit externe, comme le suggère la méthodologie du projet, car les processus mis en place pour garantir un usage responsable de la TRF sont suffisamment robustes. En effet, le programme One ID a été conçu et mis en œuvre grâce à un processus multipartite impliquant des fonctionnaires du gouvernement, l'aéroport international de Narita, des représentants des compagnies aériennes, divers fournisseurs et des experts juridiques. Selon l'aéroport, en tant qu'initiative mondiale, il est essentiel de permettre aux partenaires du projet de choisir leurs mécanismes d'application en fonction de leur culture organisationnelle.

2

Un référentiel d'audit pour valider le respect des principes d'action

Un audit du système de management de la qualité pour garantir l'utilisation responsable du TRF et valider les processus d'atténuation des risques

Cette section détaille les travaux entrepris avec AFNOR Certification pour élaborer un référentiel d'audit permettant d'attester que les organismes déployant la TRF pour la gestion des flux respectent effectivement les principes d'action. Elle présente le cadre général et son objectif, la manière dont le référentiel d'audit peut être utilisé, sa structure, et présente un extrait (le référentiel d'audit complet est figuré à l'annexe B). Cette section contient également une version mise à jour des principes d'action, revue sur la base des observations et des commentaires issus du test effectué par l'aéroport international de Narita à l'aide du questionnaire d'évaluation.

2.1 Cadre général et objectif

Fonction d'un référentiel d'audit
La fonction d'un référentiel d'audit est de servir de document de référence détaillant les exigences et les processus d'un audit pour une portée définie. En tant que tel, il peut être utilisé comme guide de bonnes pratiques, pour mener des audits internes, pour aider à formuler les besoins que les prestataires doivent satisfaire lors du développement d'un nouveau projet, ou encore pour permettre la participation à un processus de certification volontaire ou obligatoire. Généralement, les parties prenantes qui reconnaissent la nécessité d'un référentiel d'audit déterminent également la manière dont elles veulent l'utiliser. Dans le cadre de ce projet pilote, une communauté multipartite a rédigé un référentiel d'audit destiné à valider le respect des principes d'action, qui définit l'usage responsable de la TRF pour les applications de gestion des flux.

Conçu pour les applications de gestion des flux
Ce référentiel d'audit a été conçu exclusivement pour les applications de gestion des flux, c'est-à-dire les situations dans lesquelles les traits du visage d'une personne sont analysés afin d'accéder à un service, comme l'embarquement dans un avion ou l'entrée dans une salle de concert. Il est à noter que le service de reconnaissance faciale offert repose sur le consentement des utilisateurs. Ces derniers l'utilisent ainsi librement car ils le trouvent avantageux. En tant que tel, il diffère sensiblement des cas d'usage dans lesquels la reconnaissance faciale est déployée à l'insu ou sans le consentement des citoyens ou des consommateurs. Le référentiel d'audit est destiné à traiter un ensemble de questions spécifiquement liées à la gestion des flux et à valider le respect des principes d'action. Il traite des préoccupations liées à la gouvernance des données biométriques (par exemple le consentement, le respect de la vie privée), aux performances du système de reconnaissance faciale au sein de différentes catégories démographiques (par exemple l'identification et l'atténuation des biais, un seuil de performance défini) et au respect de l'autonomie des utilisateurs finaux grâce à l'expérience utilisateur (UX) du système (par exemple l'affichage des informations, le droit d'accès, la disponibilité d'une autre option). En tant que tel, il constitue le premier cadre global pour l'usage responsable de la reconnaissance faciale pour les applications de gestion des flux. Il n'est pas destiné à d'autres cas d'usage (par exemple, la surveillance de suspects dans des affaires judiciaires ou du risque de terrorisme, les achats personnalisés dans le commerce de détail, l'identification de maladies rares) et aux risques qui y sont associés.

Testé dans le cadre d'un projet pilote avant déploiement
Conformément à notre approche expérimentale, ce référentiel d'audit sera testé et révisé sur la base des résultats du pilote, en collaboration avec AFNOR Certification et les aéroports volontaires. Si les résultats sont satisfaisants, le référentiel d'audit sera alors déployé en collaboration avec des organismes de certification partenaires, à commencer par AFNOR Certification, qui a joué un rôle clé dans la conception de ce projet

Un audit du système de gestion de la qualité
Lors de l'élaboration de ce référentiel d'audit, le groupe de travail a décidé de se concentrer sur l'atténuation des risques susceptibles de provoquer une altération ou une interruption du service proposé aux utilisateurs finaux. Par exemple, lorsque l'on procède à l'embarquement de passagers dans un avion en utilisant la reconnaissance faciale, quels processus devraient être mis en place pour garantir l'égal à ce service pour tous les passagers, indépendamment de leur catégorie ethnique ou potentiel handicap qui pourrait avoir un impact sur les performances de la TRF ? Si le système est dysfonctionnel, quelles sont les alternatives raisonnables pour finaliser l'embarquement et s'assurer qu'aucun passager ne manque son vol ? Par conséquent, ce cadre est conçu pour un audit de la gestion des systèmes de reconnaissance faciale, et non de leurs algorithmes. Le groupe de travail a pris cette décision principalement parce que les utilisateurs de la technologie (par exemple, les sociétés de transport, les organisations d'événements) sont responsables de la qualité du service qu'ils fournissent à leurs clients. À cet égard, les principes d'action représentent un ensemble d'exigences qui décrivent comment un système de reconnaissance faciale de haute qualité devrait être conçu, déployé et opéré, tandis que le référentiel d'audit détaille les processus à mettre en œuvre pour garantir l'égal accès ce service aux utilisateurs finaux.

Construit dans une perspective européenne
La première version du référentiel d'audit a été rédigée dans le cadre d'une collaboration multipartite, similaire

à celle qui a été suivi pour rédiger le questionnaire d'évaluation. Une attention particulière a été portée au Règlement général sur la protection des données (RGPD) de l'UE. Les « Lignes directrices en matière d'éthique pour une IA digne de confiance » du Groupe d'experts de haut niveau sur l'intelligence artificielle de la Commission européenne ont également été prises en considération. Il s'agit d'un document essentiel qui ouvre la voie à l'utilisation éthique des technologies d'IA dans l'ensemble de l'UE. Cela signifie que les délégués à la protection des données (DPD) peuvent s'appuyer sur ce cadre, en collaboration avec leur service juridique, pour vérifier la conformité de leur TRF avec les autorités de protection des données de l'UE lorsqu'ils traitent des données de citoyens de l'UE ou lorsqu'ils opèrent dans un pays qui a obtenu un accord d'adéquation avec l'UE dans le cadre du RGPD, comme le Japon.[37] Les organisations qui utilisent la TRF pour des applications de gestion des flux mais qui ne sont pas basées dans les juridictions où le RGPD s'applique sont également encouragées à utiliser ce référentiel d'audit pour améliorer la gestion de leur système, avec pour objectif la satisfaction de leurs utilisateurs finaux. A présent, de nombreux pays et juridictions à travers le monde envisagent d'adopter des lois sur la protection des données, en s'inspirant du RGPD. Dans cette perspective, les travaux présentés dans ce livre blanc peuvent faciliter leur démarche.

Comment utiliser le référentiel d'audit

Comme mentionné, le groupe de travail multipartite a décidé d'utiliser le référentiel d'audit pour valider la conformité avec les principes d'action, qui définissent ce qu'est l'usage responsable de la TRF pour les applications de gestion des flux. Toutefois, cette validation peut prendre quatre formes différentes et complémentaires :

Guide des bonnes pratiques. Une organisation peut utiliser ce référentiel d'audit comme modèle pour concevoir et déployer son système de reconnaissance faciale de manière responsable. Dans ce cas, elle intégrerait dans le cahier des charges les spécifications que ses prestataires externes doivent respecter pendant le développement du projet.

Auto-évaluation. Une organisation qui est sur le point de déployer un système de reconnaissance faciale ou qui l'a déjà fait peut procéder à une auto-évaluation en utilisant le référentiel d'audit, de manière similaire au questionnaire d'évaluation. Toutefois, étant donné que le référentiel d'audit est plus complet, le processus d'auto-validation serait plus rigoureux.

Certification. Un tiers de confiance, idéalement un organisme de certification accrédité, peut évaluer la robustesse des processus mis en œuvre par une organisation désireuse de se conformer aux principes.

Règlement. Les décideurs politiques peuvent également adopter une législation qui exigerait que les acteurs du secteur utilisant la technologie de reconnaissance faciale pour les applications de gestion des flux soient audités. Dans ce cas, il s'agirait d'un audit statutaire.

La troisième utilisation du référentiel d'audit, la certification, est l'option qui a été retenue par le groupe travail. Elle est examinée dans les sections suivantes de ce document. Bien qu'AFNOR Certification soit le premier organisme de certification à participer à cette initiative, d'autres seront invités à rejoindre le projet pour construire un réseau d'organismes de certification capable de délivrer ce certificat à travers le monde, une fois le référentiel d'audit testé et validé.

2.2 Structure du référentiel d'audit

« la version actuelle comprend 10 principes susceptibles d'évoluer en fonction des résultats finaux du projet pilote.

Pour construire le référentiel d'audit, les principes d'action ont été détaillés en un ensemble d'exigences qui doivent être validées au cours de l'audit (décrit ci-dessous). Les exigences ont été répertoriées par critères et classées en trois types distincts.

Principes d'action

La première version des principes d'action a été présentée dans le livre blanc publié en février 2020. Ces principes ont été rédigés conjointement dans le cadre d'un processus multipartite et définissent ce qui constitue l'usage responsable de la reconnaissance faciale pour les applications de gestion des flux. Au départ, 11 principes ont été identifiés mais, pendant la phase de test, ils ont été revus et mis à jour pour garantir l'efficacité de leur mise en œuvre, leurs exhaustivités et leurs pertinences. En conséquence, la version actuelle comprend 10 principes. Néanmoins, ils sont susceptibles d'évoluer en fonction des résultats finaux du projet pilote.

1. **Utilisation proportionnelle du système de reconnaissance faciale**
   Les systèmes de reconnaissance faciale doivent être parfaitement adaptés et limités à l'usage prévu. Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures raisonnables pour évaluer les capacités et les limites des systèmes qu'ils envisagent d'utiliser et pour s'assurer que leurs systèmes sont adaptés à l'usage prévu.

2. **Évaluation des risques**
   Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'un service ou d'un système doivent réaliser une évaluation complète des risques associés à leurs systèmes, notamment leur impact sur la vie privée, le risque d'erreurs, leur prédisposition à produire des biais, leur vulnérabilité face au piratage et aux

cyberattaques, le manque de transparence du processus de prise de décisions et le risque de violation de droits civiques.

3. **Biais et discrimination**
   Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures appropriées pour garantir que tous les biais ou conséquences inéquitables (c'est-à-dire ne pas être reconnu par la TRF et bénéficier par conséquent d'un service de qualité moindre) peuvent être détectés, identifiés et atténués autant que possible. Tout en reconnaissant que l'élimination complète des biais représente l'un des défis majeurs dans le domaine de la recherche en IA, les organisations doivent allouer des ressources appropriées à la mise en œuvre d'outils et de processus qui minimisent les biais et conséquences inéquitables.

4. **Respect de la vie privée dès la conception**
   Les organisations qui utilisent des systèmes de reconnaissance faciale doivent concevoir des systèmes qui respectent la vie privée, notamment en incluant des considérations de confidentialité dans les exigences associées aux systèmes, en intégrant ce principe dans les phases de conception, de développement et de test des technologies et en favorisant les pratiques professionnelles et la maintenance continue des systèmes.

5. **Performance**
   Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'un service ou d'un système doivent respecter les critères d'évaluation de la précision et des performances de leurs systèmes aux stades de conception (tests en laboratoire) et de déploiement (tests de terrain). Ces évaluations de la performance doivent pouvoir être contrôlées par des organismes tiers compétents et leurs comptes rendus doivent être consultables par les utilisateurs des systèmes.

6. **Droit à l'information**
   Des processus doivent être mis en place pour informer les utilisateurs finaux qui ont des questions à poser et/ou recherchent des informations concernant l'utilisation des systèmes de reconnaissance faciale. Les utilisateurs finaux doivent avoir accès à leurs données biométriques personnelles sur demande.

7. **Consentement**
   Les utilisateurs finaux doivent fournir un consentement éclairé, libre, sans ambiguïté, explicite et affirmatif à propos de l'utilisation de systèmes de reconnaissance faciale. Ainsi, aucun identifiant biométrique unique ne devrait être créé et conservé sans consentement explicite. Chaque fois qu'une personne concernée souscrit un nouveau service reposant sur la TRF, elle doit exprimer clairement son consentement pour la durée de conservation des données et les conditions de stockage.

8. **Affichage de l'information**
   Lorsque ces systèmes sont utilisés dans des espaces publics, une signalisation claire doit être mise en place pour garantir une communication évidente auprès des utilisateurs finaux à propos du recours à la technologie de reconnaissance faciale. Les espaces dans lesquels des systèmes de reconnaissance faciale sont utilisés doivent toujours être délimités et indiqués. Un signal visuel doit également informer les personnes lorsque le système en question est en service.

9. **Droit d'accès aux groupes vulnérables**
   La reconnaissance faciale ne doit exclure personne et doit toujours rester accessible et utilisable par tous les groupes de personnes, y compris les personnes âgées et les personnes en situation de handicap. Il est admis que, dans certains cas, par exemple en présence de nourrissons et d'enfants, une exception à ce principe se révèle appropriée et une alternative à l'identification faciale doit être proposée.

10. **Autre option/présence humaine**
    Un examen manuel (supervision humaine) devra être réalisé chaque fois qu'une utilisation est susceptible de donner lieu à une décision portant à conséquences telle que la violation de droits civiques. Dans le cas des systèmes entièrement automatisés, un système de redondance impliquant l'intervention d'un humain doit toujours être en place pour traiter les exceptions et les erreurs possibles afin de proposer une médiation. Une alternative raisonnable aux systèmes de reconnaissance faciale doit toujours être mise en place.

Trois types d'exigences

Le respect des exigences en matière d'audit est évalué à trois étapes clés : au stade de la conception du processus, au stade de la mise en œuvre et au stade opérationnel :

– *Exigences liées aux processus introduites lors de la conception d'un système de reconnaissance faciale.* Ces exigences ont pour but d'évaluer les différents processus mis en œuvre et les ressources allouées lors de la phase de conception. L'objectif ici est de s'assurer que la conception **garantit le déploiement et l'utilisation responsable et fiable de la TRF.**

– *Exigences liées à la mise en œuvre de ces processus tout au long de l'utilisation du dispositif de reconnaissance faciale.* Ces exigences ont pour but de valider la conformité aux processus établis, leur mise en œuvre continue et leur existence à long terme une fois que le système est déployé dans une situation réelle spécifique. Il est essentiel de valider la pérennité du système et l'absence de dérives par rapport à son utilisation et aux objectifs initiaux. Ces exigences contribueront à renforcer la confiance dans l'exploitation et la gestion du système en garantissant qu'elles répondent aux attentes établies lors de la phase de conception.

– Exigences liées au fonctionnement du système. L'objectif de ces exigences est la validation du fonctionnement du système dans le respect des principes d'action. Certaines de ces exigences sont liées à celles établies lors de la phase de conception. Elles permettront de faire un arrêt sur image du système dans son fonctionnement, de valider l'expérience utilisateur et de réaliser différents tests afin de s'assurer que le système fonctionne dans le respect des principes d'action. Ces exigences permettront de valider le fonctionnement responsable du système.

2.3 Extrait du référentiel d'audit

Le référentiel d'audit complet est présenté à l'annexe B du Livre blanc, voici néanmoins un extrait pour illustrer sa structure :

– Dans la colonne de gauche, les numéros d'exigence sont indiqués.

– Dans la colonne du milieu, on trouve la description détaillée de chaque exigence.

– Dans la colonne de droite, le type d'exigence concerné est indiqué, comme décrit ci-dessus.

Utilisation proportionnelle du système de reconnaissance faciale
Exigence : Les systèmes de reconnaissance faciale doivent être parfaitement adaptés à l'usage prévu. Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures raisonnables pour évaluer les capacités et les limites des systèmes qu'elles envisagent d'utiliser et pour s'assurer que leurs systèmes sont adaptés à l'usage prévu.

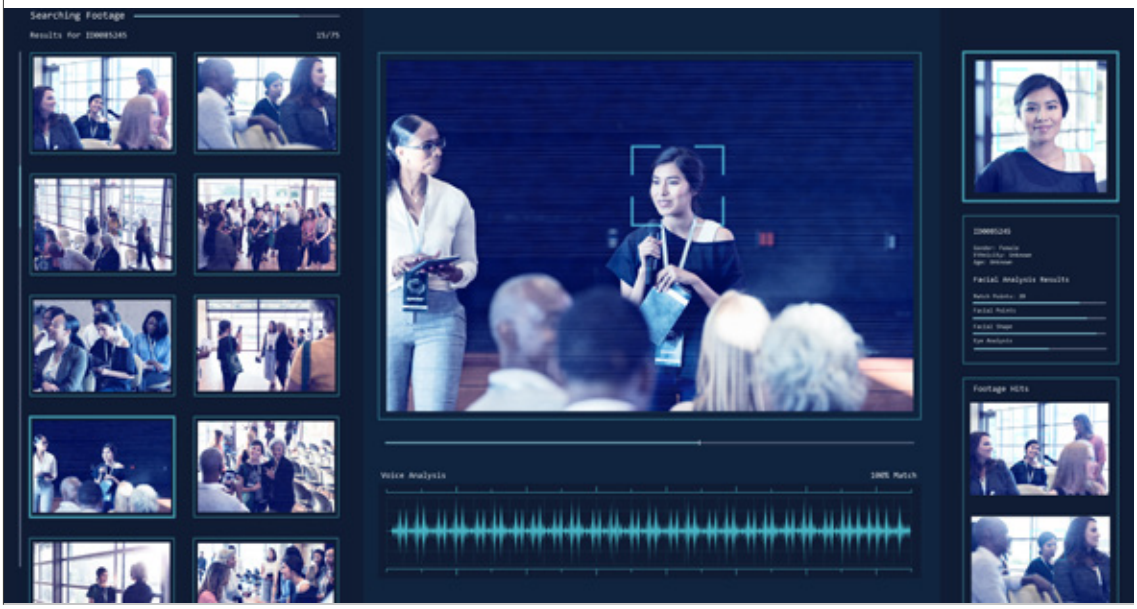
N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
1.1	En amont de tout projet de reconnaissance faciale, il faut définir le besoin qui conduit à envisager l'utilisation d'un système de reconnaissance faciale. L'entreprise doit décrire les besoins techniques pour atteindre les objectifs assignés à son système et permettre de garantir une utilisation limitée à l'usage prévu.	✓		
1.2	L'ensemble des alternatives (hors reconnaissance faciale) qui répondent au même besoin doivent être déterminées.	✓		
1.3	Pour répondre au besoin, il faut déterminer les alternatives possibles à l'utilisation d'un système de reconnaissance faciale. Un processus documenté et une méthodologie pour analyser les solutions possibles doit être mis en place. Le but est d'évaluer la pertinence de l'utilisation de la reconnaissance faciale par rapport à son objectif et la résolution du problème. Pour cela, l'entreprise détaille la méthodologie d'évaluation et de sélection qui doit comprendre à minima : – Un examen des avantages et inconvénients identifiés pour chaque solution identifiée. – Une définition des bénéfices attendus du système auprès des différentes parties prenantes (utilisateurs, État, citoyens, etc.) – Une analyse de risque sur les situations de faux positifs et de faux négatifs (notamment sur les risques de violation des droits civils) – Une évaluation quantifiée des bénéfices attendus – Une analyse comparative des différentes solutions – La conclusion qui a conduit à privilégier une solution de reconnaissance faciale.	✓		

1.4	Afin de valider les hypothèses qui ont conduit à choisir la reconnaissance faciale, l'entreprise doit définir les paramètres à respecter pour valider la pertinence de l'utilisation (exemple : taux de faux positifs et de faux négatifs attendus, performance attendue).			
1.5	Ces paramètres doivent être vérifiés dans la phase d'utilisation.			
1.6	L'utilisation de la reconnaissance faciale a été mise en place pour répondre à un besoin dans le cadre d'une utilisation bien spécifique. En fonctionnement, l'usage de la reconnaissance faciale doit être limité à celui initialement prévu et validé pour son utilisation.			

3

Un système de certification pour assurer l'usage responsable de la technologie de reconnaissance faciale pour la gestion des flux

Un schéma de certification délivré par des tiers indépendants pour garantir surveillance fiable.



Parmi les différents moyens disponibles pour valider le respect des principes d'action, le groupe de travail a décidé de se concentrer sur la certification et de s'associer avec AFNOR Certification (organisme tierce-partie). Ce tiers de confiance sera chargé d'auditer les acteurs industriels volontaires en utilisant le référentiel d'audit. Une fois que le système de certification aura été testé et validé, le groupe de travail déterminera les capacités et les compétences nécessaires pour qu'un organisme de certification puisse effectuer une évaluation de la TRF conformément au référentiel d'audit. Une fois identifiés, ces organismes seront encouragés à adopter et à gérer ce système de certification. Cette section présente le cadre général du système de certification (ses objectifs, son fonctionnement, qui est éligible, etc.) et le processus de certification en détail.

3.1 Cadre général et objectif

Fonction d'un système de certification
Les objectifs finaux d'un système de certification sont les suivants : 1) veiller à ce que le système ou le service certifié réponde à des normes de qualité prédéfinies (par exemple, efficacité, efficience, sécurité et respect des valeurs et normes sociales) ; et 2) encourager l'amélioration continue de la qualité. Il atteint ces objectifs grâce à la réalisation d'une évaluation indépendante et d'un jugement objectif sur un dispositif ou un produit donné, sur la base d'un ensemble défini d'exigences énumérées dans un référentiel d'audit. En d'autres termes, son but immédiat est de statuer sur le niveau de conformité. En tant que tel, il s'agit d'un dispositif de signalisation à la fois robuste et flexible pour les acteurs industriels qui cherchent à démontrer la fiabilité de leurs dispositifs ou systèmes. Habituellement, les organisations candidates qui s'engagent dans un tel processus poursuivent divers objectifs : améliorer leur compétitivité, promouvoir leurs bonnes pratiques, augmenter la confiance que leur accordent leurs clients et partenaires et/ou se conformer aux exigences réglementaires.

Une certification de la gestion de la qualité
Comme déjà mentionné, un audit du système de gestion de la qualité, similaire à la famille de normes ISO 9000, a été co-conçu. Par conséquent, le système de certification se concentre sur la gestion des systèmes de reconnaissance faciale pour les applications de gestion des flux et valide leur respect des principes d'action. Cependant, les différents types de certification (par exemple, produits, services, compétences professionnelles, etc.) dépassent le cadre de cette initiative. En outre, le système de certification peut prendre différentes formes selon les objectifs des organisations candidates et la demande du marché. Trois types de certification dans des domaines connexes sont présentés ci-dessous pour illustrer la manière dont le système de certification volontaire peut évoluer.

Avantages de la certification dans des domaines connexes

– *La certification en tant qu'étape nécessaire pour accéder à certains marchés :* les fournisseurs de services qui cherchent à accéder à de nouveaux marchés dans le domaine numérique, en particulier ceux qui travaillent avec de grandes organisations ou des organismes du secteur public, doivent démontrer leur capacité à sécuriser leurs systèmes d'information en étant certifiés ISO/IEC 27001. Cette certification permet aux organisations clientes de garantir la confidentialité, l'intégrité et la disponibilité des données qu'elles ont confiées à leurs fournisseurs de services grâce à la mise en œuvre de processus de sécurité des données reconnus au niveau international.

– *La certification en tant que processus volontaire autorisé par un règlement :* les organisations qui traitent les données personnelles de citoyens européens doivent se conformer au RGPD. Dans le cadre de cette obligation, elles doivent s'assurer que les sous-traitants auxquels elles confient des données à caractère personnel respectent également ce règlement. Les sous-traitants peuvent demander une certification RGPD, comme le permet l'article 42 du RGPD, afin de rassurer les contractants principaux et d'obtenir un avantage concurrentiel significatif.

– *La certification en tant que processus réglementaire :* tout organisme souhaitant fournir des services d'hébergement de données personnelles de santé pour le compte de professionnels de la santé en France doit obtenir un certificat d'hébergeur de données de santé (HDS). Cette obligation légale et sectorielle, garantit que les acteurs traitant des données sensibles, telles que les données personnelles de santé, mettent en œuvre des mesures techniques et organisationnelles pour assurer la protection de leurs données.

Qui devrait certifier ?
Une fois ce référentiel d'audit testé et validé par AFNOR Certification, l'objectif est de le mettre à la disposition d'autres organismes de certification. En outre, pour garantir l'indépendance et l'impartialité du processus de certification, les organismes de certification devront opérer conformément à la norme ISO/IEC 17021-1:2015. Cette norme contient « les principes et les exigences relatifs à la compétence, à la cohérence et à l'impartialité des organismes procédant à l'audit et à la certification de tous les types de systèmes de management ».[38] Ce point sera détaillé à l'avenir, y compris l'identification des capacités et compétences spécifiques qu'un organisme de certification devrait avoir pour mener une évaluation significative de la TRF, lorsque le système de certification sera validé.

3.2 Processus de certification

Définition du champ d'application
Le système de certification est exclusivement conçu pour les applications de gestion des flux de la TRF, exploitées par des organisations publiques ou privées. En tant que tel, le référentiel d'audit indique explicitement quels aspects de la gestion de leurs systèmes de reconnaissance faciale sont couverts par la certification et ceux qui en sont exclus.

Qui devrait être certifié ?
Toute organisation qui utilise la reconnaissance faciale pour la gestion des flux est éligible au système de certification. Elle peut en faire la demande soit au stade de la conception, lorsqu'elle commence à construire son système et réfléchit à la meilleure façon de le gérer de manière responsable, soit une fois que son système est en fonctionnement et qu'elle souhaite améliorer la qualité de sa gestion. Dans les deux cas, ce qui est demandé et évalué par l'organisme de certification est la conformité effective aux exigences du référentiel d'audit.

Qui doit payer ?
Comme il s'agit d'un système de certification volontaire pour les acteurs de l'industrie et les organisations publiques qui cherchent à s'assurer de la qualité de la gestion de leurs systèmes par le biais d'un certificat, les organisations candidates doivent prendre en charge le coût du processus de certification.

Approche d'audit de certification
L'auditeur mandaté par l'organisme de certification pour réaliser l'audit doit évaluer, sur le site, la mise en œuvre effective des processus attendus et le respect des exigences du référentiel d'audit en collaboration avec les différents services impliqués dans le processus de certification. Ce processus implique des entretiens avec les employés. En outre, les preuves de conformité au référentiel d'audit doivent être mises à disposition par l'organisation candidate pour examen par les auditeurs. Avant tout audit, l'auditeur doit fournir à l'organisation candidate des directives claires quant aux employés/fonctions susceptibles de faire l'objet d'un entretien et aux preuves de conformité qui doivent être recueillies et évaluées.

Une fois l'audit effectué, les auditeurs établissent une série d'observations qu'AFNOR Certification conseille de classer en cinq catégories :

- **Non-conformité majeure :** le non-respect d'une exigence, mettant en cause le fonctionnement, l'efficacité ou l'amélioration du système de gestion de la reconnaissance faciale
  Une non-conformité majeure doit faire l'objet d'une action corrective et doit être traitée avant que la certification puisse être délivrée.
- **Non-conformité mineure :** le non-respect d'une exigence spécifiée qui ne compromet pas en soi l'efficacité ou l'amélioration du système de gestion de la reconnaissance faciale
  Une non-conformité mineure doit faire l'objet d'une action corrective mais n'empêche pas en soi la délivrance de la certification.
- **Point sensible :** un risque latent de non-conformité
  Des preuves de conformité aux exigences du cadre de certification ont été obtenues, mais l'organisation doit modifier ses pratiques pour éliminer ce risque latent.
- **Points forts :** pratique qui dépasse le niveau de performance habituel observé en réponse aux exigences de certification
- **Remarque :** observation sur le respect des exigences du référentiel d'audit

Une fois l'audit terminé, un rapport comprenant les conclusions de l'auditeur est envoyé à l'organisation candidate. L'organisation candidate peut alors répondre à tout problème de non-conformité identifié en fournissant des documents complémentaires et le plan d'action qu'elle entend mettre en œuvre.

Décision et délivrance du certificat
Sur la base du rapport d'audit et des recommandations de l'auditeur, l'organisme de certification prend la décision de délivrer la certification et/ou de demander des vérifications supplémentaires (c'est-à-dire un audit à distance ou sur place, etc.). Le certificat est ensuite délivré pour un an, sous réserve de la mise en œuvre effective de toute action corrective décidée au cours de l'audit. Le certificat indique explicitement les aspects de la gestion de leurs systèmes de reconnaissance faciale qui entrent dans le champ d'application de la certification. Une fois certifiés, les organismes audités par AFNOR Certification sont répertoriés sur son site web.

4

Des principes à la certification : une démarche visant à renforcer la responsabilité

Un calendrier de réussite, dans lequel un audit externe est une composante de nombreuses étapes clés

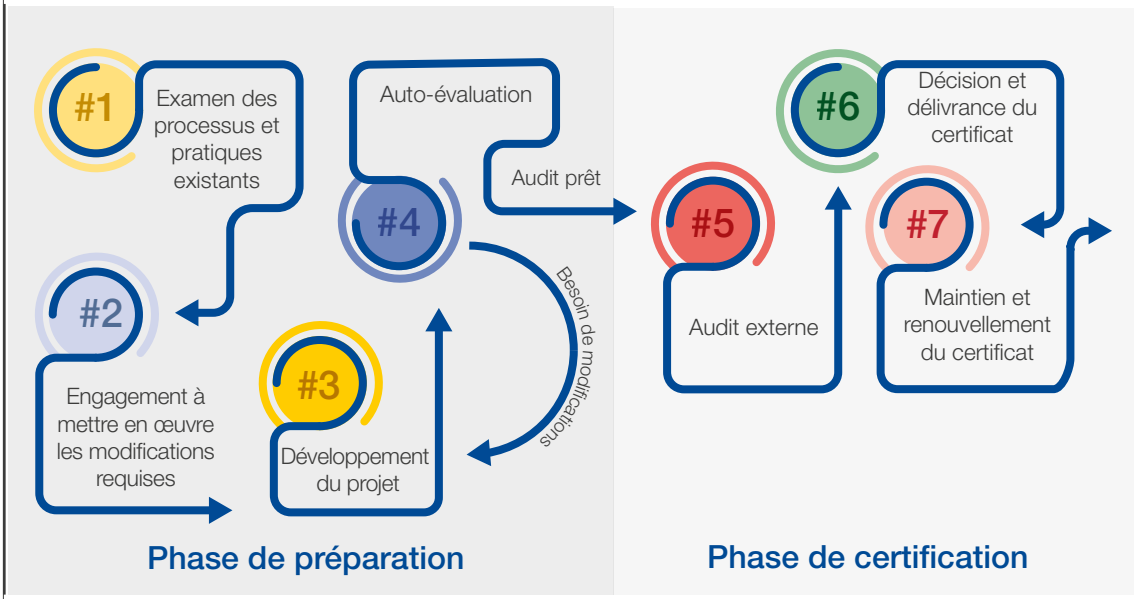
Cette certification vise à fournir un outil pratique et opérationnel pour le suivi et l'amélioration de la gestion des systèmes de reconnaissance faciale pour les applications de gestion des flux. En tant que telle, la délivrance de la certification représente une étape clé dans le parcours des organisations qui la reçoivent. On peut distinguer deux phases :

1. La phase de préparation. Les organisations qui envisagent de faire une demande de certification doivent examiner les principes d'action, mettre en œuvre les bonnes pratiques et auto-évaluer leurs processus à l'aide du questionnaire d'évaluation. Elles doivent également dresser la liste des employés susceptibles d'être interrogés et des preuves à recueillir et évaluer dans le cadre du processus de certification. Ces actions créeront les conditions d'un audit externe réussi et peu contraignant.
1. 2) La phase de certification. Les organismes accrédités évaluent formellement les processus mis en œuvre par les organisations candidates par rapport aux exigences du référentiel d'audit. Les résultats de cette évaluation déterminent la délivrance de la certification.

Pour illustrer une telle démarche, les étapes à suivre et les activités associées sont présentées dans les figures 2 et 3. Les deux scénarios possibles sont les suivants : A) les organisations offrent déjà un système de reconnaissance faciale et souhaitent obtenir une certification, ou B) les organisations ont l'intention de développer un système de reconnaissance faciale.

4.1 Une organisation propose déjà un système de reconnaissance faciale et souhaite obtenir une certification

FIGURE 2 **7 étapes pour le système de certification, lorsque le système est déjà opérationnel**



Source : Forum Économique Mondial

#1 Examen des processus et pratiques existants. Toute organisation candidate doit commencer par un examen approfondi du processus de gestion de son système de reconnaissance faciale. Ensuite, elle doit évaluer les processus et pratiques existants par rapport aux éléments du cadre de gouvernance (principes d'action, bonnes pratiques, questionnaire d'évaluation ou référentiel d'audit). Cette étape permet aux organisations de valider leur approche et de vérifier si le respect des exigences du référentiel d'audit est possible à ce stade.

- Activités à mener :
  - Un groupe de travail inter-pluridisciplinaire devra être mis en place.
  - Ce groupe de travail devrait dresser un inventaire des processus et pratiques existants afin d'évaluer s'ils sont compatibles avec les éléments du cadre de gouvernance.
  - Le groupe de travail devrait dresser l'inventaire de toutes les données/preuves qui doivent être générées, collectées et évaluées dans le cadre du processus de certification et identifier toute lacune dans la documentation ou les archives de données existantes.

- Le groupe de travail devrait signaler les lacunes identifiées à la direction, que ce soit en ce qui concerne les processus et les pratiques ou les données et les preuves utilisées pour démontrer la conformité.

#2 Engagement à mettre en œuvre les modifications requises. La direction de l'organisation candidate valide en interne la décision de passer par le processus de certification et s'engage à allouer les ressources nécessaires pour combler les lacunes identifiées :

- Activités à mener :
  - La direction de l'organisation candidate s'engage en interne à adapter ses systèmes de reconnaissance faciale pour se conformer aux exigences du référentiel d'audit.
  - La direction identifie les principales parties prenantes tant en interne (par exemple, les directeurs du conseil d'administration, les chefs d'unité, les membres du groupe de travail interservices) qu'en externe (par exemple, l'autorité nationale de protection des données).

#3 Développement du projet. L'organisation candidate met en œuvre la modification requise pour préparer le processus d'auto-évaluation.

- Activités à mener :
  - L'organisation candidate utilise le cadre de gouvernance comme modèle pour modifier ses processus et pratiques existants.

#4 Auto-évaluation. Une fois les lacunes identifiées et comblées, l'organisation candidate peut procéder à une auto-évaluation pour mesurer sa préparation au processus de certification. Cette auto-évaluation doit être menée par une équipe qui n'a pas participé à la modification des processus et pratiques problématiques afin d'éviter toute auto-validation (à noter que les résultats de l'auto-évaluation peuvent entraîner d'autres modifications). En pratique, l'organisation candidate peut avoir besoin de repasser par les étapes 2 et 3 pour affiner les processus et pratiques existants.

- Activités à mener :
  - L'organisation candidate désigne une équipe dédiée pour mener une auto-évaluation ou un audit interne.
  - L'organisation utilise le questionnaire d'évaluation et/ou le référentiel d'audit pour effectuer l'auto-évaluation.
  - L'organisation s'assure que toutes les preuves requises (données et documents) à utiliser pour appuyer la conformité sont à jour et peuvent être facilement retrouvées.
  - L'organisation informe les employés susceptibles de faire l'objet d'entretiens qu'ils peuvent être interrogés dans le cadre de l'audit (et les sensibilise à l'importance de l'audit et de leur franchise lors des entretiens dans le cadre de celui-ci).
  - L'organisation peut se comparer à d'autres organisations, telles que l'aéroport international de Narita, qui ont procédé à une auto-évaluation. (Les organisations seront encouragées à communiquer publiquement les résultats de leur questionnaire d'évaluation afin de démontrer comment un usage responsable de la TRF peut être réalisé)
- Délai indicatif :
  - L'auto-évaluation ne doit pas dépasser 1 à 2 jours et doit respecter les conditions de l'audit externe. Le délai d'analyse des écarts potentiels par rapport à la situation de référence et la mise en œuvre de mesures correctives dépendront des résultats de l'auto-évaluation.

#5 Audit externe. L'audit externe est géré par l'organisme de certification. Il se déroule en deux étapes. Tout d'abord, l'organisme de certification examine les processus que l'organisation candidate a mis en place pour se conformer aux exigences du référentiel d'audit. Pour ce faire, il examine la façon dont le système a été conçu et mis en œuvre. Ensuite, il évalue l'efficacité de ces processus en procédant à un audit du système en fonctionnement sur le site, à une date inconnue de l'organisation candidate.

- Activités à mener :
  - L'organisme de certification procédera à un audit documentaire (examen de la documentation relative à la conception et à la mise en œuvre du système).
  - L'organisme de certification effectuera un audit des activités sur le terrain (examen des procédures opérationnelles, de la documentation et des données pertinentes).
- Délai indicatif :
  - L'audit devrait prendre deux jours. Le délai dépendra du volume d'utilisateurs finaux utilisant la TRF et peut donc être prolongé en fonction du projet. En cas de duplication du système sur plusieurs sites physiques, une méthodologie d'audit par échantillonnage est mise en place.

#6 Décision et délivrance du certificat. L'organisme de certification prend sa décision sur la base des résultats de l'audit et des recommandations de l'auditeur. Il peut soit délivrer la

certification si toutes les exigences sont remplies, soit demander des mesures correctives supplémentaires. Dans le second cas, les organisations candidates auront le temps de mettre en œuvre des mesures correctives avant que l'organisme de certification ne prenne sa décision finale.

- Le certificat est valable pour une période de trois ans et est soumis à un examen basé sur un audit de suivi annuel.
- Activités à mener :
  - L'organisme de certification rédigera le rapport d'audit et publiera sa décision.
  - L'organisme de certification délivrera le certificat si les conditions sont remplies.

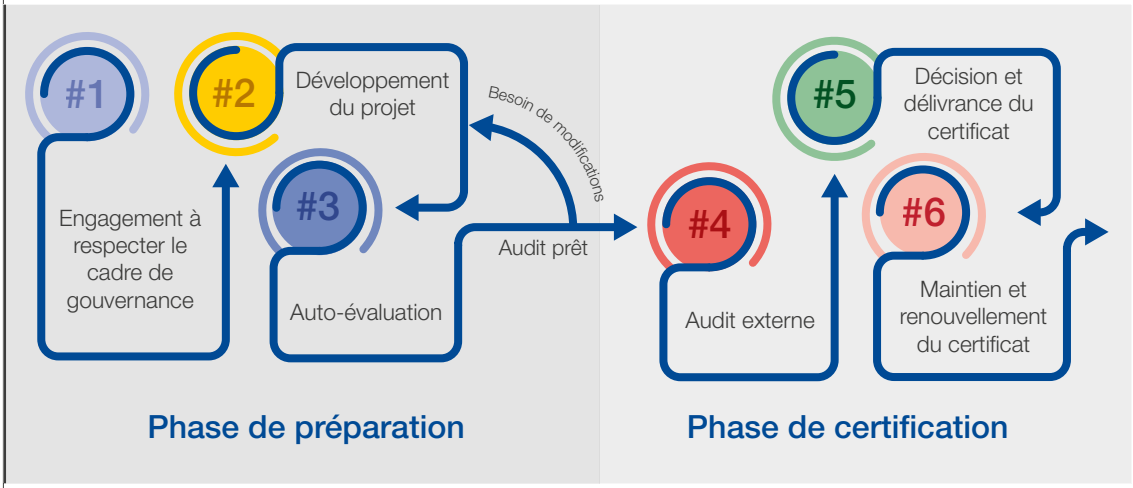
#7 Maintien et renouvellement du certificat. Un audit annuel valide le maintien des exigences. En cas de non-conformité, la certification sera retirée.

Activités à mener :

- Les audits annuels comprennent :
  - Un audit documentaire (examen de la documentation relative à la conception et à la mise en œuvre du système)
  - Un audit des activités sur le terrain (examen des procédures opérationnelles).
- Délai indicatif :
  - L'audit de maintien (suivi) devrait prendre une journée par an (la durée dépendra également des règles d'échantillonnage appliquées initialement).
  - Au bout de trois ans, un audit de renouvellement du certificat est effectué. L'audit de renouvellement devrait prendre deux jours. Le délai dépendra du volume d'utilisateurs finaux utilisant la TRF et peut donc être prolongé en fonction du projet.

4.2 Une organisation a l'intention de développer un système de reconnaissance faciale

FIGURE 3 **6 étapes pour le système de certification, lorsque le système n'est pas encore opérationnel**



Source : Forum Économique Mondial

#1 Engagement à respecter le cadre de gouvernance. L'audit se concentre sur : 1) les exigences liées aux processus introduits dans la conception d'un système de reconnaissance faciale ; 2) les exigences liées à la mise en œuvre de ces processus lorsque le système est en opération ; et 3) les exigences liées au fonctionnement du système. Par conséquent, les organisations qui examinent le cadre politique tout en concevant leurs systèmes de reconnaissance faciale auront un avantage sur celles qui gèrent un système déjà opérationnel. En effet, elles ont la possibilité de construire un système « responsable par design ».

- Activités à mener :
  - L'organisation candidate utilise le cadre de gouvernance comme modèle pour concevoir son système de gestion de la reconnaissance faciale.
  - La direction de l'organisation candidate s'engage à concevoir et à mettre en œuvre un système de reconnaissance faciale responsable, conforme aux éléments du cadre de gouvernance (y compris en garantissant que la documentation et les

données seront générées et conservées dans un endroit facilement accessible pour être utilisées dans le cadre d'un audit).

- La direction s'engagera auprès d'un organisme de certification accrédité pour délivrer ce certificat et établira un calendrier pour l'audit.

#2 Développement du projet. L'organisation candidate prépare le processus d'auto-évaluation.

- Activités à mener :
  - La direction de l'organisation candidate s'engage en interne à construire son système de reconnaissance faciale conformément aux exigences du référentiel d'audit.
  - La direction identifie les principales parties prenantes tant en interne (par exemple, les directeurs du conseil d'administration, les chefs d'unité, les membres du groupe de travail interservices) qu'en externe (par exemple, l'autorité nationale de protection des données).
  - La direction inclut les éléments du cadre de gouvernance et les exigences du référentiel d'audit dans l'ensemble des spécifications de l'auto-évaluation.

#3 Auto-évaluation. Une fois que les différents groupes de travail ont identifié et comblé les lacunes identifiées, l'organisation peut procéder à une auto-évaluation pour mesurer sa préparation au processus de certification. Cette auto-évaluation doit être menée par une équipe qui n'a pas participé à l'analyse des écarts afin d'éviter toute auto-validation (à noter que les résultats de l'auto-évaluation peuvent entraîner d'autres corrections). Dans la pratique, les parties prenantes appropriées peuvent avoir besoin d'affiner les processus et pratiques existants en conséquence.

- Activités à mener :
  - L'organisation désigne une équipe ad hoc pour mener une auto-évaluation ou un audit (exigence 2.4 du référentiel d'audit).
  - L'organisation utilise le questionnaire d'évaluation ou le référentiel d'audit pour effectuer l'auto-évaluation.
  - L'organisation peut se comparer à d'autres organisations, telles que l'aéroport international de Narita, qui ont procédé à une auto-évaluation.
- Délai indicatif :
  - L'auto-évaluation ne doit pas dépasser 1 à 2 jours et doit respecter les conditions de l'audit externe. Le délai d'analyse des écarts potentiels par rapport à la situation de référence et la mise en œuvre de mesures correctives dépendront des résultats de l'auto-évaluation.

#4 Audit externe. L'audit externe est géré par l'organisme de certification. Il se déroule en deux étapes. Tout d'abord, l'organisme de certification examine les processus que l'organisation candidate a mis en place pour se conformer aux exigences du référentiel d'audit. Pour ce faire, il examine la façon dont le système a été conçu et mis en œuvre. Ensuite, il évalue l'efficacité de ces processus en procédant à un audit du système en fonctionnement sur le site, à une date inconnue de l'organisation candidate.

- Activités à mener :
  - L'organisme de certification procédera à un audit documentaire (examen de la documentation relative à la conception et à la mise en œuvre du système).
  - L'organisme de certification effectuera un audit des activités sur le terrain (examen des procédures opérationnelles).
- Délai indicatif :
  - Durée indicative de l'audit : 2 jours. Le délai dépendra du volume d'utilisateurs finaux utilisant la TRF et peut donc être prolongé en fonction du projet. En cas de duplication du système sur plusieurs sites physiques, une méthodologie d'audit par échantillonnage est mise en place.

#5 Décision et délivrance du certificat. L'organisme de certification prend sa décision sur la base des résultats de l'audit et des recommandations de l'auditeur. Il peut soit délivrer la certification si toutes les exigences sont remplies, soit demander des mesures correctives supplémentaires. Dans le second cas, les organisations candidates auront le temps de mettre en œuvre des mesures correctives avant que l'organisme de certification ne prenne sa décision finale.

- Activités à mener :
  - L'organisme de certification rédigera le rapport d'audit et publiera sa décision.
  - L'organisme de certification délivrera le certificat si les conditions sont remplies.

#6 Maintien et renouvellement du certificat. Un audit annuel valide le maintien des exigences. En cas de non-conformité, la certification sera retirée.

- Activités à mener :
  - Les audits annuels comprennent :
    - Un audit documentaire (examen de la documentation relative à la conception et à la mise en œuvre du système)

  - Un audit des activités sur le terrain (examen des procédures opérationnelles).

- Délai indicatif :

  - L'audit de maintien (suivi). Durée indicative de l'audit : 1 jour par an (la durée dépendra également des règles d'échantillonnage appliquées initialement).
  - Au bout de trois ans, un audit de renouvellement du certificat est effectué. Durée indicative de l'audit de renouvellement : 2 jours. Le délai dépendra du volume d'utilisateurs finaux utilisant la TRF et peut donc être prolongé en fonction du projet.

4.3 Conséquences d'une non-conformité majeure

Le système de certification étant fondé sur la base du volontariat, en cas de non-conformité mineure, les entreprises disposent d'un mois pour apporter les corrections nécessaires. Toutefois, si les auditeurs constatent une non-conformité majeure, la certification est retirée. En conséquence, les entreprises doivent immédiatement cesser de communiquer des informations sur la certification et peuvent être invitées à informer publiquement leurs consommateurs qu'elles ne détiennent plus la certification.

Si le modèle de certification volontaire est intégré dans un texte de loi, les cas majeurs de non-conformité seront alors traités de manière beaucoup plus conséquente :

- La loi peut imposer l'arrêt immédiat du système de reconnaissance faciale jusqu'à ce que les problèmes identifiés soient entièrement résolus. L'organisme de certification suspend le certificat pendant cette période pour le réactiver ultérieurement, le cas échéant.
- La loi peut autoriser l'utilisation du système de reconnaissance faciale problématique pendant une période définie au cours de laquelle l'entreprise doit résoudre les problèmes identifiés. Si l'entreprise parvient à les résoudre , l'organisme de certification ne suspend pas le certificat. Toutefois, si l'entreprise n'est pas en mesure de résoudre les problèmes, le système est mis à l'arrêt et le certificat est retiré.

La législation doit préciser à la fois le type de problèmes majeurs de non-conformité qui nécessitent un arrêt immédiat du système de reconnaissance faciale et la procédure que l'entreprise doit suivre pour reprendre ses activités une fois les problèmes réglés.

5

Conclusion

Un schéma de certification est la réponse réglementaire appropriée pour les cas d'utilisation de la gestion des flux.

“ En cas de succès, ce projet pilote ouvrira la voie à la conception d’un cadre de gouvernance pour l’application responsable des systèmes de reconnaissance faciale.

A travers le monde, de nombreuses organisations de la société civile ont pris conscience des risques potentiels associés à la TRF et exhortent les élus à agir pour les atténuer, car l’influence de cette technologie sur la société se développe rapidement. Certains décideurs politiques aux États-Unis et dans l’Union européenne ont entendu cet appel et reconnaissent le besoin urgent de créer un cadre de gouvernance robuste. Toutefois, il n’existe pas de consensus sur la voie à suivre.

Ce Livre blanc démontre qu’un système de certification est la réponse réglementaire appropriée pour les cas d’usage de la gestion des flux. En effet, confier à un organisme de certification comme AFNOR Certification le soin d’évaluer le respect des principes d’action est un moyen souple et efficace de garantir la conception et l’utilisation responsable de la TRF pour les applications de gestion des flux.

Les acteurs industriels ou organisations publiques qui souhaitent recourir à la certification pour démontrer la gestion responsable de leurs dispositifs de reconnaissance faciale doivent passer par un processus rigoureux et structuré en plusieurs étapes qui commence par un examen du cadre de gouvernance (principes d’action, bonnes pratiques, questionnaire d’évaluation et référentiel d’audit), qui peut servir de guide pour concevoir ou améliorer un système de reconnaissance faciale existant. Toutefois, ce processus ne s’achève pas avec la délivrance du certificat. En effet, avoir un dispositif digne de confiance implique un effort d’évaluation itératif et continu. Par conséquent, le groupe de travail espère qu’à long terme, les organismes certifiés contribueront à développer une culture organisationnelle qui favorisera l’identification et l’atténuation des risques en constante évolution, au profit des utilisateurs de la technologie, des clients et de la société dans son ensemble.

Les gouvernements ont un rôle clé à jouer dans la promotion de cette culture. Aussi, une fois que le projet pilote sera achevé et les résultats jugés concluants, les élus seront encouragés à prendre en considération les propositions du présent Livre blanc et à adopter une législation rendant cette certification obligatoire pour les acteurs de l’industrie qui utilisent la TRF pour des applications de gestion des flux.

Les prochaines étapes de ce projet pilote consistent à tester le référentiel d’audit et le système de certification avec les acteurs industriels, à évaluer leur pertinence et la charge de travail qu’ils créent pour les organisations candidates, et à les examiner sur la base des résultats observés. En cas de succès, ce projet pilote ouvrira la voie à la conception d’un cadre de gouvernance pour l’application responsable des systèmes de reconnaissance faciale. Une fois le projet pilote terminé, une coalition d’acteurs multipartites s’engageant à respecter et à promouvoir ce modèle de certification sera formée.

Les acteurs industriels, les acteurs publics, les représentants de la société civile, les organismes de certification, les décideurs politiques et les universitaires sont encouragés à rejoindre cette initiative et à participer pour renforcer ce modèle de certification et garantir sa réussite.

La méthodologie appliquée pour ce projet, basée sur des cas d’usage, pourrait servir de modèle aux acteurs industriels désireux de garantir l’usage responsable de la TRF dans d’autres cas d’usages. En tant que tel, il contient des enseignements importants. Par conséquent les organisations intéressées par le déploiement de cette méthode dans d’autres cas d’usage sont invitées à contacter le Centre pour la quatrième révolution industrielle du Forum Économique Mondial.

Glossaire

Précision de la reconnaissance faciale : la précision d'un système de reconnaissance faciale repose sur l'association de deux éléments : 1) la fréquence à laquelle le système identifie correctement une personne inscrite dans le système ; et 2) la fréquence à laquelle le système ne trouve aucune correspondance pour une personne non inscrite. Ces deux conditions, appelées « vraies » conditions, s'associent à deux « fausses » conditions pour décrire toutes les conséquences possibles d'un système de reconnaissance faciale (cf. définitions des termes Vrai positif, Vrai négatif, Faux positif et Faux négatif).

Algorithme : série d'instructions d'exécution d'un calcul ou de résolution d'un problème, en particulier à l'aide d'un ordinateur. Ces instructions forment le fondement de toutes les opérations réalisables par un ordinateur et, par conséquent, constituent un aspect fondamental de tous les systèmes d'IA.

Audit : la fonction essentielle d'un audit est de servir de document de référence qui détaille les exigences et les processus d'un audit pour une portée définie.

Biométrie : la biométrie s'applique à diverses technologies qui utilisent à des fins d'identification et d'authentification les attributs identifiables uniques des personnes, y compris (mais sans s'y limiter) les empreintes digitales, l'empreinte de l'iris, l'empreinte de la main, le modèle de visage, l'empreinte vocale, la démarche ou la signature d'une personne.

Certification : la fonction essentielle d'un système de certification est d'effectuer une évaluation indépendante afin d'obtenir un jugement objectif sur un système ou un produit donné, sur la base d'un ensemble défini d'exigences énumérées dans un référentiel d'audit.

Vision par ordinateur : la vision par ordinateur est un domaine de l'informatique qui vise à permettre aux ordinateurs de voir, d'identifier et de traiter des images à la manière d'un humain, puis de produire un résultat approprié.

Inscription : l'inscription désigne le processus d'inscription d'images de personnes de manière à créer des gabarits permettant de les reconnaître. Lorsqu'une personne est inscrite dans un système de vérification utilisé à des fins d'authentification, son gabarit est également associé à un identifiant principal qui servira à déterminer le gabarit à comparer avec le gabarit d'exploration.

Explicabilité : propriété des systèmes d'IA permettant de fournir une forme d'explication de la démarche empruntée pour parvenir à des conclusions, afin d'améliorer la compréhension des décisions prises ainsi que la confiance des opérateurs et utilisateurs de ces systèmes.

Détection faciale : répond à la question « Cette image comporte-t-elle un ou plusieurs visages humains ? » La détection identifie les visages humains.

Identification faciale (ou un pour plusieurs) : répond à la question « Cette personne inconnue peut-elle être mise en correspondance avec un gabarit inscrit ? » Cette identification compare un gabarit d'exploration avec tous les gabarits d'inscription stockés dans un référentiel, c'est pourquoi elle est également appelée correspondance « un pour plusieurs », ou one-to-many en anglais. Les correspondances entre candidats sont produites en fonction du degré de concordance entre le gabarit d'exploration et chacun des gabarits inscrits.

Vérification faciale (ou un pour un) : répond à la question « Ces deux images représentent-elles la même personne ? » En situation de sécurité ou d'accès, cette vérification s'appuie sur l'existence d'un identifiant principal (tel que la pièce d'identité d'un client) et la reconnaissance faciale est utilisée en second lieu pour vérifier l'identité de la personne. Cette vérification est également appelée correspondance « un pour un » ou one-to-one en anglais, car le gabarit d'exploration (une personne) est comparé uniquement au gabarit stocké pour la (une) personne associée à l'identification présentée.

Reconnaissance faciale : application logicielle biométrique capable d'opérer une identification ou vérification exclusive d'une personne en comparant et en analysant les caractéristiques de cette personne en fonction de ses lignes faciales.

Faux négatif : résultat de test qui indique, de manière erronée, que la personne représentée dans l'image d'exploration n'est pas inscrite et qu'il n'y a pas de correspondance, alors qu'elle est bien inscrite. Selon le cas d'usage de la reconnaissance faciale, les conséquences des faux positifs peuvent varier considérablement.

Faux positif : résultat de test qui indique, de manière erronée, que la personne représentée dans l'image d'exploration est inscrite dans le système, alors qu'elle ne l'est pas. Selon le cas d'usage de la reconnaissance faciale, les conséquences des faux positifs peuvent varier considérablement.

Image d'exploration : une image d'exploration est une image soumise à un système de reconnaissance faciale pour être comparée à des personnes inscrites. Les images d'exploration sont également converties en gabarits d'exploration. Comme pour les gabarits d'inscription, des images de bonne qualité donnent lieu à des gabarits de bonne qualité.

Gabarit : les images des personnes sont converties en gabarits, qui servent ensuite à la reconnaissance faciale. Des caractéristiques pouvant être interprétées par ordinateur sont extraites d'une ou plusieurs images d'une personne pour créer le gabarit de cette personne.

Vrai négatif : la personne représentée dans l'image d'exploration n'est pas inscrite et il n'y a pas de correspondance.

Vrai positif : la personne représentée dans l'image d'exploration est inscrite et il y a une correspondance correcte.

Contributeurs

Auteurs principaux

Ichirou Akimoto
Cadre supérieur, développement commercial de l'IA à l'international, NEC Corporation, Japon ; membre du Forum Économique Mondial

Yusuke Inoue
Japanese Government Fellow, Forum Économique Mondial, Centre pour la quatrième révolution industrielle du Japon

Sebastien Louradour
French Government Fellow, Forum Économique Mondial

Lofred Madzou
Directeur de projet AI/ML, Forum Économique Mondial

Jérémie Mella
Chef de projets, AFNOR Certification, France

Communauté du projet

Le Forum Économique Mondial remercie les membres de la communauté du projet pour leur analyse et leurs commentaires :

Didier Baichère
Membre de l'Assemblée nationale, France

Xavier Blondeau
Responsable du programme de vidéosurveillance, SNCF, France

Vincent Bouatou
Directeur du Laboratoire d'innovation, IDEMIA, France

Pascal Briand
Manager IT, Traitement des passagers, Groupe ADP, France

Laurent Dahmani
Directeur-Général adjoint, AFNOR Certification, France

Jean-Luc Dugelay
Professeur d'ingénierie et de sécurité numérique, EURECOM, France

Marine Dunoguier
Directrice des systèmes embarqués, Alcatraz, États-Unis

Rosanna Fanni
Chercheuse en éthique de l'IA, Belgique

Louis-Thomas Fernandes
Expert LAF, SNCF, France

Romain Galesne-Fontaine
Directeur des relations institutionnelles et de la communication externe, IN Groupe, France

Hervé Genty
Responsable de la sécurité des données retail, SNCF, France

Brice Gilbert
Chef de projets, cybersécurité, AFNOR Certification, France

Ilana Golbin
Directrice, Technologies émergentes et IA responsable, PwC, États-Unis

Bruce Hedin
Directeur Scientifique, H5, États-Unis

Matissa Hollister
Professeure adjointe de comportement organisationnel, Université McGill, Canada ; Research Fellow, Forum Économique Mondial

Luc Julia
Vice-président Senior et Directeur technique, Samsung Strategy and Innovation Center, Samsung Electronics, République de Corée

Eva Kaili
Membre du Parlement européen

Brenda Leong
Conseillère principale et directrice, Intelligence artificielle et éthique, Future of Privacy Forum, États-Unis

Gautier Martin
Chef de projets, Développement de Services et Produits Aéroportuaires, Groupe ADP, France

Hidehisa Matsumoto
Senior Manager, Corporate Strategies Office, Narita International Airport Corporation, Japon

Franck Maurin
Directeur des produits et solutions de facilitation du traitement des passagers et des contrôles aux frontières, IDEMIA, France

Cédric Mazière
Responsable du programme de vidéosurveillance, SNCF, France

Michaël Mesure
Directeur LAF, SNCF, France

Shaun Moore
Directeur général et co-fondateur, Trueface, États-Unis

Anand Rao
Responsable mondial du département IA, PwC, USA

Arthur Ribemont
Chef de projets, Confiance numérique, AFNOR Certification, France

Mathieu Rondel
Directeur Expertise et Performance Opérationnelle, Direction des Opérations Aéroportuaires, Groupe ADP, France

Stéphane Séjourné
Membre du Parlement européen

Karen Silverman
Fondatrice et Directrice générale du groupe Cantellus, États-Unis

Emilia Tantar
Chief Data and Artificial Intelligence Officer, Black Swan LUX, Luxembourg

Isabelle Valverde
Responsable de la gestion des flux, SNCF, France

Philippe Weiss
Responsable du projet de reconnaissance faciale, SNCF, France

Tomohiro Yamane
Directeur, Politiques publiques et recherche pour l'innovation de l'aviation, Division des affaires générales, Bureau de l'aviation civile, Ministère japonais de l'intérieur, des infrastructures du transport et du tourisme.

Nous tenons également à remercier la CNIL pour son intervention en qualité d'observateur indépendant, et plus particulièrement :

Marie Duboys Fresney
Juriste

Félicien Vallet
Ingénieur

Annexes

Annexe A : Réponses de l'aéroport international de Tokyo-Narita au questionnaire d'évaluation

1. Utilisation proportionnelle du système de reconnaissance faciale

Questions d'évaluation	Réponses (auto-évaluation de l'aéroport international de Narita)
Quelles sont les alternatives à votre système de reconnaissance faciale ? Pourquoi les avez-vous rejetées ? Quels sont les critères utilisés pour déterminer les avantages et les inconvénients de ces alternatives ?	La reconnaissance des empreintes digitales et de l'iris sont considérées comme des alternatives. La comparaison a permis de déterminer que la reconnaissance faciale était préférable pour les raisons suivantes : 1. Son aspect pratique, les passagers n'ont pas besoin d'utiliser un équipement 2. Son utilisation sans contact s'est avérée utile lors de la pandémie de COVID-19 3. Une donnée unique pour identifier une personne et qui peut être collectée sans manipulation particulière 4. Le concept de cadence de marche normale peut être réalisé
Comment avez-vous évalué la pertinence de votre système par rapport à son objectif ?	Elle a été évaluée sur la base des trois points suivants : 1. Grande précision de la reconnaissance faciale 2. Satisfaction des exigences des utilisateurs finaux (compagnies aériennes) 3. Analyse de la performance, notamment pour les situations spécifiques telles que la cadence de marche
Décrivez les exigences techniques pour atteindre les objectifs de votre système dans un format compréhensible par les autorités compétentes.	Les principaux points sont les suivants : 1. Précision de la reconnaissance faciale 2. Cadence de marche normale 3. Compatibilité avec les systèmes existants des compagnies aériennes en cours de déploiement (pas besoin de modifications importantes du système) 4. Conformité aux normes IATA
Avez-vous mené une analyse de risque sur les situations de faux positifs et de faux négatifs (notamment sur les risques de violation des droits civils) ?	Nous avons analysé le risque d'erreur d'embarquement et d'autres facteurs avec un comité tiers (Comité de protection des données, MLIT qui inclut des avocats, des professeurs d'université et des groupes de consommateurs).

2. Évaluation des risques

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Avez-vous évalué rigoureusement les risques liés à l'utilisation de votre système avant (par exemple, cadre d'évaluation) et pendant son fonctionnement opérationnel (par exemple, référentiel d'audit) en utilisant les dimensions suivantes ?	
Vie privée	Ce risque a été évalué par un comité tiers (Comité de protection des données, MLIT qui inclut des avocats, des professeurs d'université et des groupes de consommateurs).

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Erreurs	Nous avons mis en place des fonctions de contrôle et de détection des erreurs du système pour permettre aux utilisateurs du système (compagnies aériennes, etc.) et aux propriétaires du système (aéroport international de Narita) de déterminer les erreurs.
Biais	Ce risque a été évalué par un comité tiers (Comité de protection des données, MLIT : y compris des avocats, des professeurs d'université et des groupes de consommateurs).
Piratage et cyberattaques	Nous avons réalisé un contrôle intitulé « Security by Design », une évaluation du système par un tiers, et nous avons effectué des tests de réponses aux cyber-attaques, etc.
Transparence dans le processus de prise de décision	Le processus d'approbation a été mené par l'autorité compétente sur la base du contrat. Nous avons également organisé une réunion de coordination visant à déterminer les spécifications du système avec les utilisateurs du système (compagnies aériennes, etc.).
Violation des droits de l'homme et des droits civils	Ce risque a été évalué par un comité tiers (Comité de protection des données, MLIT : y compris des avocats, des professeurs d'université et des groupes de consommateurs).

3. Biais et discrimination

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Comment définissez-vous les biais dans votre cas d'usage ? Décrivez les mesures utilisées pour évaluer chacun d'entre eux.	Nous avons adopté un système de reconnaissance faciale parce que le circuit intégré (CI) du passeport contient des informations faciales et parce que ce système a été utilisé dans d'autres aéroports. Nous avons défini les biais comme des différences de performances (mesures : précision et temps de certification) entre personnes d'ethnies différentes et en situation de handicap, telles que les personnes en fauteuil roulant. Toutefois, les personnes dont le passeport ne comporte pas de CI ou dont le pays ne permet pas d'accéder a un tel service ne sont pas éligibles.
Quel est votre cadre d'analyse des risques ? Décrivez les risques de biais identifiés pour votre cas d'usage et les groupes représentés par les caractéristiques des utilisateurs finaux concernés par les biais que vous avez évalués.	Nous avons utilisé le JIS Q 31000 basé sur la norme ISO 31000 comme cadre d'analyse des risques pour l'ensemble du système. En ce qui concerne l'évaluation des biais, nous avons demandé aux fournisseurs de soumettre les résultats de l'examen public mené par le NIST, etc. comme élément de vérification du système de reconnaissance faciale.
Comment les risques sont-ils classés par ordre de priorité dans ce processus ? Comment les intérêts concurrents sont-ils résolus ?	La disponibilité et la sécurité de l'ensemble du système ont été considérées comme une priorité absolue. Les fonctions individuelles ont été examinées en fonction de leur impact sur l'ensemble du système.
Veuillez décrire les bonnes pratiques existantes pour la détection, l'identification et l'atténuation des biais qui ont été appliquées dans ce cas.	Nous avons passé en revue les fournisseurs de reconnaissance faciale dans NISTIR 8280 et avons sélectionné le fournisseur doté des meilleurs algorithmes au moment où nous avons pris notre décision.
Quels plans d'action avez-vous mis en place pour atténuer les principaux risques identifiés ? Pour chaque risque de biais, quelles mesures d'atténuation ont été identifiées et comment ont-elles été évaluées pour en garantir l'efficacité ?	En ce qui concerne l'évaluation des biais, nous avons demandé aux fournisseurs de soumettre les résultats de l'examen public mené par le NIST, etc. comme élément de vérification du système de reconnaissance faciale. Le système de NEC étant le plus précis au moment où nous avons pris notre décision, nous avons décidé de le sélectionner.
Quels sont les cas d'essai et les tests d'acceptation utilisés pour votre système de reconnaissance faciale ?	Nous avons effectué des tests d'acceptance (y compris des tests opérationnels prenant en compte l'environnement lumineux local) pour respecter les conditions du cas d'usage. Nous avons demandé aux fournisseurs de soumettre les résultats de l'examen public mené par le NIST, etc., comme élément de vérification du système de reconnaissance faciale.

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Comment est réparti l'ensemble de votre formation et dans quelle mesure s'aligne-t-elle sur celle des utilisateurs finaux de votre système ? S'il y a des lacunes, comment avez-vous évalué leur impact et comment y avez-vous remédié ?	Nous avons conçu des cas d'usage, testé (acceptance du système) et créé des scénarios d'entrainement avec les compagnies aériennes utilisatrices. Nous avons demandé aux fournisseurs de soumettre les résultats de l'examen public mené par le NIST, etc., comme élément de vérification du système de reconnaissance faciale.
Quels sont les compromis auxquels vous êtes confrontés lors du déploiement de votre système ? Comment les abordez-vous ?	Nous devons réaliser des arbitrages entre protection des données personnelles et simplicité d'utilisation, etc. La protection des données personnelles est gérée selon un processus multipartite.
Si vous avez été confrontés à des écarts entre les critères de validation et les performances réelles, comment ces écarts ont-ils été atténués ?	Pour réduire l'altération de la précision de la reconnaissance faciale due à la lumière du soleil, nous avons pris des mesures physiques supplémentaires, comme des films opacifiants et des rideaux, et avons ajusté le logiciel, comme le paramètre de reconnaissance faciale, pour qu'il soit conforme aux exigences.

4. Respect de la vie privée dès la conception

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Quels processus (par exemple, un groupe de travail) et ressources (par exemple, une charte des bonnes pratiques) avez-vous mis en œuvre pour favoriser la protection de la vie privée des personnes concernées, par exemple pour éviter la collecte excessive de données biométriques par rapport aux finalités de l'utilisation ?	En travaillant avec le bureau de protection des données personnelles et le conseiller juridique de l'entreprise, nous avons identifié les problèmes juridiques, établi la direction à suivre pour mettre en place les solutions, et avons participé à des discussions avec le Bureau de l'aviation civile et le Comité de protection des données personnelles. Par la suite, le Bureau de l'aviation civile a mis en place un groupe d'experts (comité tiers) et a introduit un processus multipartite pour traiter les questions relatives à la protection des données personnelles. Un guide a été préparé sur la base de l'expansion nationale du programme One ID, tout en évitant les critiques.
Avez-vous créé un poste de responsable de la protection des données ?	En ce qui concerne le système de protection des données personnelles, un règlement interne avait déjà été établi avant le début de ce projet, et un responsable a été désigné conformément à ce règlement.
Comment encouragez-vous une collaboration étroite lors de la phase de développement de votre système de reconnaissance faciale, y compris avec les chefs de produits, l'équipe juridique, les concepteurs UX, les data scientists et développeurs de données, afin de garantir un niveau élevé de protection des données ?	Nous avons réalisé un contrôle intitulé « Security by Design », une évaluation du système par un tiers, et nous avons effectué des tests de réponses aux cyber attaques, etc.

5. Performance

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Pour les essais en laboratoire et sur le terrain, quelles normes existantes (par exemple, l'Organisation internationale de normalisation [ISO], AFNOR Certification et le Comité européen de normalisation [CEN]) suivez-vous pour évaluer la précision et les performances de votre système ? Quels critères ont été utilisés pour choisir les normes et standards que vous suivez ?	La dernière version des produits NEC qui est conforme aux normes biométriques de l'ISO/IEC JTC 1/SC 37 est utilisée pour le seul système de reconnaissance faciale.
Avez-vous soumis votre système de reconnaissance faciale au National Institute of Standards and Technology (NIST) pour évaluation ?	Nous avons utilisé l'évaluation du NIST (IR 8271) comme référence.
Quel processus avez-vous mis en place pour garantir le caractère auditable des résultats de votre système de reconnaissance faciale ? Quelles mesures ont été prises pour permettre un audit suffisant par un tiers ?	Sur la base des exigences de performance en matière de cadence de marche, des tests du système (tests fonctionnels, non fonctionnels : disponibilité, fiabilité, performance et tests biométriques) ont été effectués et vérifiés.
Quelle est la pertinence des tests de performance effectués concernant le cas d'usage considéré ?	Ils sont pertinents. Nous avons effectué un test de mise en œuvre à la porte d'embarquement, qui a nécessité une capacité de traitement supérieure à celle d'un avion classique de 250 passagers, à trois voies pendant 15 minutes. Vérification des économies de main-d'œuvre et de la réduction du personnel au sol par rapport au fonctionnement actuel.
Comment justifiez-vous le seuil de performance choisi qui induit un taux théorique de faux positifs et un taux mesuré de faux négatifs ?	Nous nous conformons aux spécifications des portiques de reconnaissance faciale requises par l'Agence des services d'immigration du Ministère de la Justice.

6. Droit à l'information

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Quels processus ont été mis en place pour tenir les utilisateurs finaux informés de l'utilisation de votre système et de leurs données biométriques ? En outre, quels processus, y compris les moyens d'escalade et de résolution, ont été mis en œuvre pour les situations où il est estimé que le système a causé un préjudice ? Les bonnes pratiques comprennent, sans s'y limiter, l'assistance aux clients et les services de renseignements.	Nous nous conformons au guide « Guidebook on the handling of personal data in One ID services that utilize facial recognition technology at airports » du Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme et nous le présentons aux utilisateurs. Adresse électronique : voir ci-dessus Numéro de téléphone : voir ci-dessus FAQ sur l'assistance aux clients : voir ci-dessus Chatbot d'assistance aux clients : non prévu.

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Une personne concernée pourrait-elle accéder, récupérer ou demander la suppression de données personnelles (photo, vidéo, données biométriques rattachées à l'identité de la personne, telles que l'historique des événements du compte, l'historique des consentements, l'historique de l'effacement des données biométriques, les informations partagées, l'historique de l'utilisation des données biométriques) dans un format lisible et dans un délai raisonnable (par exemple pas plus de 30 jours) ?	Les données sont supprimées dans les 24 heures.
Avez-vous établi et rendu publics (par exemple sur votre site web) les principes de gouvernance qui guident la conception et l'utilisation de votre système dans un format intelligible pour les non-experts ?	Ils seront publiés sur le site web, dans des brochures, etc.
Avez-vous mis en place un processus permettant aux personnes d'accéder de manière anonyme à des informations pertinentes sur le fonctionnement du système ?	Non.

7. Consentement

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
La politique de consentement fournit-elle des informations explicites et claires aux utilisateurs, et plus précisément :	Il est clairement indiqué sur l'écran au moment de l'enregistrement. Les informations sont également disponibles sur le site web et sur des affiches placées dans le terminal.
La page de consentement est-elle accessible au maximum après 2 clics et facilement visible dans la page « profil » ?	Il suffit d'un clic. Pour afficher les règles, il faut faire défiler la même page. L'annulation d'une opération avant la fin de la procédure ne génère pas de jeton. La page de profil n'est pas affichée.
Un résumé des dispositions clés est-il accessible sur cette même page ?	Oui.
Ce résumé contient-il les informations suivantes ?	
Description de l'ensemble des finalités prévues	Oui.
Durée de conservation des données	Oui.
Politique de partage des données (y compris avec quels tiers ces données vont être partagées)	Oui.
Moyen mis en place pour protéger, sécuriser et stocker les données.	Oui.

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Ce résumé est-il synthétique, lisible pour des non-experts et moins long que l'équivalent de deux pages format A4 ?	Oui.
La page permettant de donner ou de ne pas donner son consentement permet-elle aux utilisateurs de l'indiquer pour chacun des objectifs existants ?	Aucun jeton n'est généré si l'utilisateur n'est pas d'accord avec tout.
Toutes ces options sont-elles sur la même page ?	Oui.
La liste des objectifs existants est-elle à jour ?	Elle est à jour.

8. Affichage de l'information

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Quels moyens ont été mis en place pour informer les personnes qu'elles pénètrent dans une zone où un système de reconnaissance faciale est utilisé ? Ces moyens sont-ils suffisamment visibles et explicites pour le public ? Un affichage de rappel des droits des utilisateurs est-il en place ?	La zone de reconnaissance faciale et la zone générale sont clairement distinguées par l'utilisation d'un logo spécial indiquant la reconnaissance faciale, etc. Nous nous conformons au guide « Guidebook on the handling of personal data in One ID services that utilize facial recognition technology at airports » du Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme et nous le présentons aux utilisateurs : affiches, panneaux, etc. dans l'aéroport.
Pour l'accès aux locaux, la gestion des flux et/ou l'inscription dans un espace public, le volume de la zone d'enregistrement ne dépasse-t-il pas l'espace de capture défini et identifié par les utilisateurs ? Comment vous assurez-vous que l'espace de capture est compris par les utilisateurs finaux (veuillez fournir des preuves basées sur l'évaluation/la recherche/les tests) ?	Nous vérifions le système de reconnaissance faciale au moment de son déploiement pour nous assurer qu'il ne dépasse pas l'espace de capture.
Un affichage de taille suffisante permet-il de relayer l'objectif du système de reconnaissance faciale ? Comment vous assurez-vous que l'affichage est visible et lisible (veuillez fournir des preuves basées sur l'évaluation/la recherche/les tests) ?	Un logo et un code de couleurs destinés à la reconnaissance faciale sont utilisés pour accroître la visibilité et rendre l'affichage reconnaissable quelle que soit sa taille.

9. Droit d'accès aux groupes vulnérables

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Pouvez-vous détailler comment le système a été conçu et évalué pour soutenir les personnes âgées et les personnes souffrant de handicap (y compris visuel etw auditif) ?	Nous nous conformons au guide « Guidebook on the handling of personal data in One ID services that utilize facial recognition technology at airports » du Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme et nous le présentons aux utilisateurs : affiches, panneaux, etc. dans l'aéroport.
Votre système de reconnaissance faciale est-il accessible à tous, y compris aux personnes âgées et aux personnes souffrant de handicap ?	Accessible. Cependant, le sujet doit se trouver à une hauteur comprise entre 130 et 190 cm pour que les appareils photo puissent prendre des images.
Quelles ressources avez-vous allouées à l'aide aux personnes âgées et aux personnes souffrant de handicap ?	Nous avons affecté du personnel (personnel de l'aéroport et des compagnies aériennes) à chaque point de contact.
Pour les personnes souffrant de handicap, les enfants, les familles et les autres personnes pour lesquelles le système ne fonctionne pas ou n'est pas souhaitable, il peut être utile de recourir à une autre solution ayant été testée et validée.	Nous mettons à disposition un personnel ad hoc (personnel de l'aéroport et des compagnies aériennes) pour faire face à ce type de situation.

10. Autre option/présence humaine

Questions d'évaluation	Réponses à l'auto-évaluation de l'aéroport international de Narita
Avez-vous mis en place un processus d'examen manuel pour les situations dans lesquelles la concordance d'un visage et d'une pièce d'identité dotée d'une photo conduit à un faux négatif, notamment lors de la phase d'inscription ?	Il n'y a pas de processus d'examen manuel. L'automatisation complète et l'élimination des faux négatifs sont réalisées grâce à l'ajout d'un service Cloud qui renvoie les informations à la compagnie aérienne hôte pour la vérification des informations sur les passagers, les passeports, etc. En cas d'erreur, un processus manuel similaire à l'opération en cours doit être effectué par une personne.
Pour les systèmes de reconnaissance faciale, l'option alternative est-elle mise en place et :	Mise en place : nous remplaçons le fonctionnement manuel actuel par du personnel.
exécutée par des agents humains ? (Ces opérateurs sont-ils formés pour gérer des situations exceptionnelles ?)	Nous remplaçons le fonctionnement manuel actuel par du personnel.
raisonnable, c'est-à-dire qu'elle n'entraîne pas de conséquences négatives disproportionnées (par exemple, le temps nécessaire pour passer le contrôle de sécurité deux fois plus long) ?	Elle peut être utilisée comme un système équivalent à celui qui existe déjà et peut être réalisée dans le même temps de traitement qu'auparavant.
Existe-t-il un processus alternatif pour les personnes qui n'acceptent pas l'utilisation de leurs données biométriques ?	Il peut être utilisé comme un système équivalent à celui qui existe déjà. Les opérations manuelles constituent un processus alternatif.

Annexe B: Référentiel d'audit

1. Utilisation proportionnelle du système de reconnaissance faciale

Exigence :

Les systèmes de reconnaissance faciale doivent être parfaitement adaptés et limités à l'usage prévu. Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures raisonnables pour évaluer les capacités et les limites des systèmes qu'ils envisagent d'utiliser et pour s'assurer que leurs systèmes sont adaptés à l'usage prévu.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
1.1	En amont de tout projet de reconnaissance faciale, il faut définir le besoin qui conduit à envisager l'utilisation d'un système de reconnaissance faciale. L'entreprise doit décrire les besoins techniques pour atteindre les objectifs assignés à son système et permettre de garantir une utilisation limitée à l'usage prévu.	✓		
1.2	Détermination de l'ensemble des alternatives (hors reconnaissance faciale) qui répondent au même besoin.	✓		
1.3	Pour répondre au besoin, il faut déterminer les alternatives possibles à l'utilisation d'un système de reconnaissance faciale. Un processus documenté et une méthodologie pour analyser les solutions possibles doit être mis en place. L'objectif est d'évaluer la pertinence de l'utilisation de la reconnaissance faciale par rapport à son objectif et la résolution du problème. Pour cela, l'entreprise détaille la méthodologie d'évaluation et de sélection qui doit comprendre à minima : – Une revue des avantages et inconvénients identifiés pour chaque solution identifiée. – Une définition des bénéfices attendus du système auprès des différentes parties prenantes (utilisateurs, Etat, citoyens, etc.) – Une analyse de risque sur les situations de faux positifs et de faux négatifs (notamment sur les risques de violation des droits civils) – Une évaluation quantifiée des bénéfices attendus. – Une analyse comparative des différentes solutions – La conclusion qui a conduit à privilégier une solution de reconnaissance faciale	✓		
1.4	Afin de valider les hypothèses qui ont conduit à choisir la reconnaissance faciale, l'entreprise doit définir les paramètres à respecter pour valider la pertinence de l'utilisation (exemple : taux de faux positifs et de faux négatifs attendus, performance attendue).	✓		
1.5	Ces paramètres doivent être vérifiés dans la phase d'utilisation		✓	
1.6	L'utilisation de la reconnaissance faciale a été mise en place pour répondre à un besoin dans le cadre d'une utilisation bien spécifique. En fonctionnement, l'usage de la reconnaissance faciale doit être limité à celui initialement prévu et validé pour son utilisation.			✓

2. Évaluation des risques

Exigence :

Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'un service ou d'un système doivent réaliser une évaluation complète des risques associés à leurs systèmes, notamment leur impact sur la vie privée, le risque d'erreurs, leur prédisposition à produire des biais, leur vulnérabilité face au piratage et aux cyberattaques, le manque de transparence du processus de prise de décisions et le risque de violation de droits civiques.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
2.1	Réalisation de l'évaluation complète des risques du système de reconnaissance faciale. L'analyse doit prendre en compte les points suivants : – Impact sur la vie privée, – Potentiel d'erreurs, – Susceptibilité d'un biais, – Vulnérabilité aux cyberattaques (piratages, ransomware, etc.), – Manque de transparence dans le processus documenté de prise de décision, – Violation potentielle des droits civils. L'analyse doit également permettre de classer les solutions mises en œuvre pour atténuer les risques.	✓		
2.2	L'analyse des risques doit la mise en place d'un plan de traitement des risques L'analyse doit également permettre de classer les risques et les solutions mises en œuvre pour les atténuer.	✓		
2.3	Les actions issues du plan de traitement de l'analyse des risques doivent être mises en œuvre et maintenues. Des indicateurs permettant d'évaluer leur efficacité et leur maintien en condition opérationnelle doivent être mis en place.		✓	✓
2.4	L'utilisateur de la technologie de reconnaissance faciale doit mettre en place des dispositifs pour s'assurer qu'il déploie son projet dans le respect des principes d'action. Pour cela, il doit réaliser une des actions suivantes : – Une auto-évaluation sur la base du questionnaire d'évaluation – Un audit interne sur la base du présent référentiel. Les conclusions et livrables qui en découlent doivent être accessibles. Ils valident notamment le déploiement du système en intégrant les recommandations. L'auditeur tiers devra avoir accès à la méthodologie employée. Cette démarche devra également être effectuée pendant le fonctionnement du système pour s'assurer du respect des principes d'action.	✓		

3. Biais et discrimination

Exigence :

Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures appropriées pour garantir que tous les biais ou conséquences inéquitables (c'est-à-dire ne pas être reconnu par la TRF et bénéficier par conséquent d'un service de qualité moindre) peuvent être détectés, identifiés et atténués autant que possible. Tout en reconnaissant que l'élimination complète des biais représente l'un des défis majeurs dans le domaine de la recherche en IA, les organisations doivent allouer des ressources appropriées à la mise en œuvre d'outils et de processus qui minimisent les biais et conséquences inéquitables.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
3.1	Mise en place d'une définition des biais dans le périmètre de votre utilisation de la reconnaissance faciale. Il faut notamment réaliser une revue des biais (exemple en annexe)	✓		
3.2	Description des bonnes pratiques qui ont été appliquées à votre cas d'usage pour détecter, identifier et atténuer les biais.	✓		
3.3	Réalisation d'un cahier des charges à destination des fournisseurs. Le cahier des charges doit être réalisé à partir d'une évaluation des risques documentés, afin de prendre les mesures appropriées pour garantir que l'ensemble des risques (dont les biais) ou des conséquences inéquitables peuvent être détectés, identifiés et atténués autant que possible. L'évaluation doit à minima inclure les points suivants et présentés en annexe : – Description des risques de biais identifiés pour votre cas d'usage et les caractéristiques des groupes d'utilisateurs finaux qui pourraient subir ces risques de biais. – Définition des caractéristiques des utilisateurs finaux du système, en tenant par exemple compte des tranches d'âge, du sexe, de l'origine ethnique, et les réunir en priorisant les groupes qui nécessitent une attention particulière en raison des risques de biais dont ils peuvent faire l'objet. – Prise en compte des accessoires et éléments pouvant impacter l'algorithme : lunettes de soleil, chapeaux, barbes, masques, etc. Le cahier des charges doit également tenir compte de ces situations. – Mise en place de paramètres pour évaluer chacun des biais identifiés aux différentes étapes du processus d'utilisation. Ces paramètres permettront notamment de hiérarchiser les risques de biais. – Chaque étape du processus d'utilisation (par exemple, en observant les biais basés sur la capture d'image et les biais basés sur les performances du modèle) doit être analysée pour identifier et évaluer les risques de biais associés. – Hiérarchisation des risques de biais et traitements des intérêts divergents	✓		

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
3.4	Concernant les risques relevant de l'utilisation du système, il faut pouvoir définir et documenter la façon dont les risques identifiés seront atténués. La mise en place de processus et de ressources pour garantir que les résultats potentiellement discriminant soient détectés et atténués de la meilleure façon possible lors de l'utilisation de la technologie (exemple en annexe) est nécessaire.	✓	✓	
3.5	Pour chaque risque de discrimination identifié, il faut déterminer l'évaluation de la performance du système de reconnaissance faciale pour atténuer ce biais avec les précisions sur les paramètres utilisés et systèmes de mesures (modèle annexe 4). Mise en place d'indicateurs pour évaluer et valider l'efficacité des stratégies Ces évaluations devront se réaliser en conception et durant le fonctionnement du système afin de valider le respect des indicateurs.	✓	✓	
3.6	Mise en place d'actions correctives et d'atténuation lors du fonctionnement du système lorsque des dérives sur les biais sont identifiés par rapport aux objectifs.		✓	✓
3.7	Réalisation de tests du système biométrique ainsi que la mise en place d'un cahier de recette pour valider l'algorithme	✓	✓	
3.8	Détermination de la distribution de vos données d'entraînement et mesure des points similaires/différents à celle des utilisateurs du système. S'il existe des écarts, il faut évaluer les impacts et les réduire.	✓		
3.9	Identification et description des arbitrages pour vos clients/utilisateurs (ex : arbitrages entre avantages et inconvénients produits par la technologie). Mise en place d'un processus de résolution des arbitrages lorsque des intérêts divergents apparaissent.	✓	✓	
3.10	Mise en œuvre de processus et de ressources (déterminé en 1.4) pour garantir que les situations potentiellement discriminantes soient détectées et atténuées durant l'utilisation du système de la meilleure façon possible pour réduire l'impact utilisateur. Concernant les risques relevant de l'utilisation du système, des actions permettant d'atténuer les risques doivent être mises en place.		✓	✓
3.11	Des critères permettant de déterminer que le système est prêt pour un déploiement et utilisation doit être mis en place (exemple performance du système, situations discriminantes…). En phase d'utilisation, il faut s'assurer du respect de ces critères.	✓		

4. Respect de la vie privée dès la conception

Exigence :

Les organisations qui utilisent des systèmes de reconnaissance faciale doivent concevoir des systèmes qui respectent la vie privée, notamment en incluant des considérations de confidentialité dans les exigences associées aux systèmes, en intégrant ce principe dans les phases de conception, de développement et de test des technologies et en favorisant les pratiques professionnelles et la maintenance continue des systèmes.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
4.1	L'entreprise se doit de respecter les normes et réglementation en vigueur sur la protection des données personnelles.	✓		
4.2	Mise en place d'un processus documenté et de ressources pour assurer la confidentialité des données biométriques. Le processus doit être déployé et maintenu dans l'utilisation du système.	✓	✓	
4.3	Mise en place de formation des équipes au développement de produits de reconnaissance faciale respectant nativement la vie privée (notamment les chefs de produit, l'équipe juridique, les concepteurs UX, les data scientists et les développeurs) pour assurer un niveau élevé de protection des données.	✓		

5. Performance

Exigence :

Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'un service ou d'un système doivent respecter les critères d'évaluation de la précision et des performances de leurs systèmes aux stades de conception (tests en laboratoire) et de déploiement (tests de terrain). Ces évaluations de la performance doivent pouvoir être contrôlées par des organismes tiers compétents et leurs comptes rendus doivent être consultables par les utilisateurs des systèmes.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
5.1	L'utilisateur de la technologie s'assure auprès de son fournisseur que la construction de la base de données ad hoc ou accessible via API comprend des échantillons suffisamment égaux des sous-groupes qui composent la population d'utilisateurs finaux et de collecter les données en conséquence. Pour cela, il met à disposition de son fournisseur les caractéristiques des utilisateurs finaux. Le fournisseur doit déterminer les critères qui l'ont conduit à choisir sa méthode d'évaluation et les standards et normes qui ont permis de choisir le logiciel. Ces points sont partis intégrantes du cahier des charges pour la sélection du système.	✓		

5.2	Le fournisseur de la technologie doit apporter les éléments qui permettent de valider l'attente du seuil de performance demandé dans le cahier des charges par l'utilisateur	✓		
5.3	Démontrer et valider que le seuil de performance choisi (qui induit un taux théorique de faux positifs et un taux mesuré de faux négatifs) est respecté dans le fonctionnement du système		✓	✓
5.4	Les évaluations du fonctionnement et leurs comptes-rendus sont contrôlables et consultables par des tierces parties indépendantes.		✓	
5.5	Mise en place de processus pour que les évaluations de performance soient auditables. Des mesures doivent être prises pour permettre un audit suffisant de ces résultats par un auditeur.	✓	✓	

6. Droit à l'information

Exigence :

Des processus doivent être mis en place pour informer les utilisateurs finaux qui ont des questions à poser et/ou recherchent des informations concernant l'utilisation des systèmes de reconnaissance faciale. Les utilisateurs finaux doivent avoir accès à leurs données biométriques personnelles sur demande.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
6.1	Mise en place d'un processus documenté pour tenir les utilisateurs finaux informés de l'utilisation du système et de l'utilisation de leurs données biométriques. Le processus doit pouvoir intégrer les évolutions sur l'utilisation du système pour en informer les utilisateurs.	✓		
6.2	Le dispositif d'information aux utilisateurs finaux sur l'utilisation du système et leurs données biométriques doit être pérenne et tenir compte des évolutions du système et de l'utilisation des données biométriques.		✓	
6.3	Les utilisateurs doivent avoir accès aux informations sur l'utilisation de leurs données biométriques. Les informations sur l'utilisation des données biométriques sont à jour.			✓
6.4	Mise en place de processus documenté (par exemple, procédures d'escalade et de résolution) pour traiter les cas de préjudice subi par les utilisateurs.	✓		
6.5	L'utilisateur doit pouvoir déclarer un préjudice. Les meilleures pratiques incluent, mais ne sont pas limitées à la mise à disposition : D'une adresse e-mail D'un numéro de téléphone D'une FAQ d'assistance client D'un chatbot d'assistance client			✓
6.6	Traçabilité et traitement des cas de préjudices communiqués par les utilisateurs		✓	

6.7	Disposition permettant aux utilisateurs d'accéder, récupérer, et demander la suppression des données personnelles (photo, vidéo, données biométriques rattachées à l'identité de la personne : historique des événements du compte, historique des consentements, historique de l'effacement des données biométriques, informations partagées, historiques de l'utilisation des données biométriques) dans un format lisible et dans un délai raisonnable (par exemple 30 jours).	✓		✓
6.8	Traçabilité et mise en œuvre des demandes d'accès, récupération et suppression des données personnelles		✓	
6.9	Mise en place d'un processus permettant aux individus d'accéder anonymement aux informations pertinentes sur le fonctionnement du système.	✓		✓
6.10	Communication au public (par exemple sur son site Web) des principes de gouvernance qui guident la conception et l'utilisation du système dans des formes intelligibles pour les non-experts.			✓
6.11	Les informations pertinentes sur le fonctionnement du système doivent être publiques et accessibles.			✓

7. Consentement

Exigence :

Les utilisateurs finaux doivent fournir un consentement éclairé, libre, sans ambiguïté, explicite et affirmatif à propos de l'utilisation de systèmes de reconnaissance faciale. Ainsi, aucun identifiant biométrique unique ne devrait être créé et conservé sans consentement explicite. Chaque fois qu'une personne concernée souscrit un nouveau service reposant sur la TRF, elle doit exprimer clairement son consentement pour la durée de conservation des données et les conditions de stockage.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
7.1	Définition des dispositions qui seront mise en œuvre pour le consentement afin de garantir que les utilisateurs puissent donner un consentement éclairé, explicite et affirmatif à propos de l'utilisation du système de reconnaissance faciale.	✓		

7.2	La politique de consentement doit être disponible en ligne et fournir des informations explicites et claires aux utilisateurs, à savoir :
	– La page de consentement doit être accessible au maximum après 2 clics et est facilement visible dans la page « profil »
	– Un résumé des dispositions clés est accessible dans cette même page. Celui-ci doit contenir les informations suivantes :
	  – Description de l'ensemble des finalités prévues,
	  – Durée de conservation des données,
	  – Politique de partage des données (notamment avec quels tiers ces données vont être partagées),
	  – Moyen mis en place pour protéger, sécuriser et stocker les données.
	– Ce résumé doit être synthétique, lisible pour des personnes non expertes et ne pas dépasser l'équivalent de deux pages format A4.
				✓

7.3	La page web de consentement doit permettre d'apporter ou de retirer son consentement pour chacune des finalités existantes. Toutes ces options doivent être sur la même page.			✓
7.4	A chaque souscription, l'utilisateur doit exprimer clairement son consentement pour la durée de conservation des données.			✓
7.5	L'entreprise doit être en capacité de fournir les éléments nécessaires pour démontrer que chaque utilisateur a exprimé clairement son consentement lors d'un audit tierce partie.		✓	
7.6	L'entreprise doit s'assurer que les dispositions concernant le consentement sont pérennes et accessibles pour les utilisateurs.		✓	
7.7	En cas d'évolution du service de reconnaissance faciale, la liste des finalités existantes doit être à jour et communiquée de façon explicite aux utilisateurs finaux Des dispositions doivent être mises en place pour inclure les évolutions.		✓	✓

8. Affichage de l'information

Exigence :

Lorsque ces systèmes sont utilisés dans des espaces publics, une signalisation claire doit être mise en place pour garantir une communication évidente auprès des utilisateurs finaux à propos du recours à la technologie de reconnaissance faciale. Les espaces dans lesquels des systèmes de reconnaissance faciale sont utilisés doivent toujours être délimités et indiqués. Un signal visuel doit également informer les personnes lorsque le système en question est en service.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
8.1	Conception du système d'information et de communication sur l'utilisation de la reconnaissance faciale dans le respect de l'exigence avec prise en compte de : L'information des utilisateurs et des noms des utilisateurs (ce qui doit être communiqué, par quel moyen...) de l'utilisation de la reconnaissance faciale et sur la zone où le système de reconnaissance faciale est utilisé Une méthodologie pour déterminer la zone où le système de reconnaissance faciale doit être mis en place.	✓		
8.2	L'ensemble des dispositifs d'information doit être mise en place, comprenant : Une information claire pour les individus qui entrent dans une zone où le système de reconnaissance faciale est utilisé. Ce moyen doit être suffisamment visible et explicite pour les individus. Un signal (visuel par exemple) doit informer les personnes lorsque le système en question est en service. L'affichage de rappel de droits de l'utilisateur est mis en place. La présence d'un affichage de taille suffisante permettant de rappeler la finalité du dispositif de reconnaissance faciale.			✓

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
8.3	Disposition pour s'assurer que la zone de capture est clairement comprise par les utilisateurs.		✓	
8.4	L'affichage de l'information doit être pérenne. Des dispositions pour s'en assurer doivent être mises en place.		✓	

9. Droit d'accès aux groupes vulnérables

Exigence :

La reconnaissance faciale ne doit exclure personne et doit toujours rester accessible et utilisable par tous les groupes de personnes, y compris les personnes âgées et les personnes en situation de handicap. Il est admis que, dans certains cas, par exemple en présence de nourrissons et d'enfants, une exception à ce principe se révèle appropriée et une alternative à l'identification faciale doit être proposée.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
9.1	Description de la façon dont le système a été définie et évalué pour n'exclure personne, y compris pour les personnes âgées et/ou en situation d'handicap (notamment visuels ou auditifs). Il faudra préciser si le système de reconnaissance faciale est accessible aux personnes âgées et les personnes handicapées.	✓		
9.2	Le périmètre prévu d'utilisateur du système de reconnaissance faciale devra être effectif dans le fonctionnement. Il faudra également évaluer si le périmètre d'utilisateur est cohérent ou si une solution alternative devient pertinente (gestion des situations rencontrées).		✓	✓
9.3	Définition des cas où il est admis, qu'une exception à ce principe se révèle appropriée et une alternative à la reconnaissance faciale doit être proposée. Il sera nécessaire de décrire les ressources allouées pour accompagner les personnes âgées et les personnes handicapées	✓		
9.4	Description et mise en place de l'option alternative pour les nourrissons, les enfants et leurs familles	✓		✓
9.5	Les dispositions pour que le système n'exclut personne doivent être déployées. Il sera nécessaire d'évaluer son efficacité et de le rendre pérenne (mise en œuvre de la solution alternative).		✓	✓

10. Autre option/présence humaine

Exigence :

Un examen manuel (supervision humaine) devra être réalisé chaque fois qu'une utilisation est susceptible de donner lieu à une décision portant à conséquences telle que la violation de droits civiques. Dans le cas des systèmes entièrement automatisés, un système de redondance impliquant l'intervention d'un humain doit toujours être en place pour traiter les exceptions et les erreurs possibles afin de proposer une médiation. Une alternative raisonnable aux systèmes de reconnaissance faciale doit toujours être mise en place.

N° Exigence	Descriptif de l'exigence du référentiel	Exigences de processus liées à la		Exigences liées au fonctionnement du système
		conception	mise en œuvre	
10.1	Identification des situations susceptible de donner lieu à une décision portant à conséquence telle que la violation de droits civiques (situations ou le rapprochement entre un visage et un document d'identité comportant une photo entraine un faux négatif, notamment au cours de la phase d'enrôlement).	✓		
10.2	Mise en place d'un processus d'examen manuel pour éviter toute situation de préjudice pour les utilisateurs.	✓		✓
10.3	Ce processus doit être mis en place et maintenu dans le fonctionnement du système.		✓	✓
10.4	Mise en place d'un processus alternatif avec identification des cas qui l'utiliseront (les nourrissons, les enfants et leurs familles par exemple). Cette alternative devra également tenir compte des personnes qui n'acceptent pas l'utilisation de leur biométrie.	✓		
10.5	Pour les systèmes de reconnaissance faciale, l'option alternative doit être mise en place et être : Opérée par des agents humains. (Ces opérateurs doivent être formés pour gérer les situations d'exception) Raisonnable ; à savoir qu'elle n'entraîne pas de conséquences négatives disproportionnées (par exemple, doubler le temps nécessaire pour passer le contrôle de sécurité).			✓
10.6	Afin de garantir que l'option alternative n'entraine pas de conséquences négatives, il faut effectuer : Une analyse de l'efficacité du dispositif et amélioration du système Traçabilité du taux d'utilisation de l'examen manuel Prise en compte des situations où une décision portant à conséquence telle que la violation de droits civiques a été rencontrée.		✓	

Annexe B1 : Définition des risques

N° risque	Risques identifiés	Description du risque	Cause du risque

Annexe B2 : Analyse de risques

N° biais	Risque identifiés	Caractéristiques du groupe d'utilisateurs finaux	Etape du processus d'utilisation où le risque sera rencontré	Paramètres d'évaluation des risques						Classification du risque
-	-	-	-	Impact utilisateur		Discrimination		Droit civique		Scoring du risque
				Gravité	Probabilité d'occurrence	Gravité	Probabilité d'occurrence	Gravité	Probabilité d'occurrence	Niveau de gravite potentielle
N°1 -	- A compléter	- A compléter	- A compléter	A compléter		A compléter		A compléter		Choisissez un élément.
				Choisissez un élément.	Choisissez un élément.	Choisissez un élément.	Choisissez un élément.	Choisissez un élément.	Choisissez un élément.	Choisissez un élément.

Définition des critères (indicateurs) qui permettent d'identifier le niveau de risque.

Niveau de Risque :	Probabilité d'occurrence :
– Très forte = A définir	– Très fréquent = A définir
– Forte = A définir	– Fréquent = A définir
– Moyenne = A définir	– Moyenne = A définir
– Faible = A définir	– Faible = A définir

Annexe B3 : Stratégies d'atténuation

Numéro du risque	Risque identifiés	Stratégie d'atténuation du risque		Indicateur pour mesurer la performance de la stratégie	Bénéfice de la stratégie d'atténuation sur le système
		Conception	Utilisation		

Annexe B4 : Système de détection des risques

Numéro du risque	Risques identifiés	Système de détection du risque	Mesure des indicateurs en fonctionnement pour évaluer l'efficacité de la détection		
		Mise en place d'indicateur permettant d'évaluer l'efficacité des stratégies	I1 :	I2 :	I3 :
		I1 I2 I3			

Endnotes

1. Shankland, Stephen, “Tokyo 2020 Olympics using facial recognition system from NEC, Intel”, CNET, 1er octobre 2019, https://www.cnet.com/news/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel (consulté le 1er octobre 2020).
2. McGinnis, Chris, “Facial recognition is coming to domestic air travel”, SFGATE, 8 septembre 2020, https://www.sfgate.com/travel/article/Facial-recognition-domestic-flights-15550415.php (consulté le 2 octobre 2020).
3. Ouvert en 1978, l’aéroport international de Narita (code de l’aéroport : NRT) propose des vols vers plus de 140 destinations intérieures et internationales. Il gère environ 258 000 décollages et atterrissages par an. Voir le site web de l’aéroport international de Narita à l’adresse suivante https://www.naa.jp/jp pour plus d’informations.
4. NEC, “NEC to provide facial recognition system for new ‘One ID’ check-in to boarding process at Narita Airport”, Communiqué de presse, 28 février 2019, https://www.nec.com/en/press/201902/global_20190228_01.html (consulté le 2 octobre 2020).
5. Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme, “Guidebook on the handling of personal data in One ID services that utilize face recognition technology at airports”, 13 mars 2020, https://www.mlit.go.jp/report/press/kouku19_hh_000096.html (consulté le 2 octobre 2020).
6. Forum Économique Mondial, “Cadre d’action pour un usage responsable de la reconnaissance faciale - Cas d’usage : gestion des flux”, Livre blanc, février 2020, http://www3.weforum.org/docs/WEF_Cadre_d’action_Reconnaissance_Faciale_2020.pdf (consulté le 1er octobre 2020).
7. Harwell, Drew et Geoffrey A. Fowler, “U.S. Customs and Border Protection Says Photos of Travelers Were taken in a Data Breach”, The Washington Post, 11 juin 2019, https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach (consulté le 2 octobre 2020).
8. Ibid.
9. Manancourt, Vincent, “Controversial US facial recognition technology likely illegal, EU body says”, Politico, 10 juin 2020, https://www.politico.eu/article/clearview-ai-use-likely-illegal-says-eu-data-protection-watchdog (consulté le 1er octobre 2020).
10. Burton-Harris, Victoria et Philip Mayor, “Wrongfully Arrested Because Face Recognition Can’t Tell Black People Apart”, American Civil Liberties Union, 24 juin 2020, https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart (consulté le 2 octobre 2020).
11. Conger, Kate, Richard Fausset et Serge F. Kovaleski, “San Francisco Bans Facial Recognition Technology”, The New York Times, 14 mai 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (consulté le 2 octobre 2020).
12. Ravani, Sarah, “Oakland bans use of facial recognition technology, citing bias concerns”, San Francisco Chronicle, 17 juillet 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php (consulté le 2 octobre 2020).
13. DeCosta-Klipa, Nik, “Boston City Council unanimously passes ban on facial recognition technology”, Boston Globe, 24 juin 2020, https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban (consulté le 2 octobre 2020).
14. Ruckstuhl, Laney, “Brookline Passes Ban On Municipal Use Of Facial Recognition Tech”, WBUR News, 12 décembre 2019, https://www.wbur.org/news/2019/12/12/brookline-facial-recognition-technology-ban (consulté le 2 octobre 2020).
15. DeCosta-Klipa, Nik, “Cambridge becomes the largest Massachusetts city to ban facial recognition”, Boston Globe, 14 janvier 2020, https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition (consulté le 2 octobre 2020).
16. Cote, Jackson, “Northampton bans facial recognition technology, becoming third community in Massachusetts to do so”, Mass Live, mise à jour du 27 février 2020, https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html (consulté le 2 octobre 2020).
17. NBC Boston, “Boston Approves Ban on Facial Recognition Technology”, 24 juin 2020, https://www.nbcboston.com/news/local/boston-approves-ban-on-facial-recognition-technology/2148450 (consulté le 2 octobre 2020).
18. Peters, Jay, “Portland passes strongest facial recognition ban in the US”, The Verge, 9 septembre 2020, https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology (consulté le 2 octobre 2020).

19. État de Washington, “Engrossed Substitute Senate Bill 6280”, 66e législature, session ordinaire de 2020, 12 mars 2020, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate Passed Legislature/6280-S.PL.pdf?q=20200331083729 (consulté le 2 octobre 2020).
20. Gouvernement du Congrès, “S.4084 - Facial Recognition and Biometric Technology Moratorium Act of 2020”, 116e Congrès (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/4084/text?r=1&s=1 (consulté le 2 octobre 2020).
21. Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications, septembre 2018, https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf (consulté le 2 octobre 2020).
22. American Civil Liberties Union, “Coalition Letter Calling for a Federal Moratorium on Face Recognition”, 3 juin 2019, https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition (consulté le 2 octobre 2020).
23. Learned-Miller, Erik, Vicente Ordóñez, Jamie Morgenstern et Joy Buolamwini, Facial Recognition Technologies in the Wild: A Call for a Federal Office, Ligue pour la justice algorithmique, 29 mai 2020, https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_TRFsFederalOfficeMay2020.pdf (consulté le 2 octobre 2020).
24. Duffy, Clare, “Microsoft president calls for federal regulation of facial recognition technology”, CNN Business, 18 juin 2020, https://edition.cnn.com/2020/06/18/tech/brad-smith-microsoft-facial-recognition/index.html (consulté le 2 octobre 2020).
25. The Amazon blog, “We are implementing a one-year moratorium on police use of Rekognition”, 10 juin 2020, https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition (consulté le 2 octobre 2020).
26. Peters, Jay, “IBM will no longer offer, develop, or research facial recognition technology”, The Verge, 8 juin 2020, https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software (consulté le 2 octobre 2020).
27. Commission européenne, “Intelligence artificielle - Une approche européenne axée sur l’excellence et la confiance”, COM(2020) 65 final, 19 février 2020, https://op.europa.eu/fr/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1/language-fr (consulté le 2 octobre 2020).
28. Espinoza, Javier et Madhumita Murgia, “EU backs away from call for blanket ban on facial recognition tech”, Financial Times, 11 février 2020, https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5 (consulté le 2 octobre 2020).
29. Ministère de la Justice du Japon, “Further Use of Facial Recognition Automated Gates (Notice)”, http://www.moj.go.jp/ENGLISH/m_nyuukokukanri07_00016.html (consulté le 6 octobre 2020).
30. Le National Institute of Standards and Technology (NIST) (Institut national des normes et de la technologie) est un laboratoire de sciences physiques et une agence non réglementaire du département du commerce des États-Unis. Parmi ses diverses activités, il procède régulièrement à l’évaluation des performances des solutions de reconnaissance faciale de fournisseurs privés, d’organisations publiques et d’institutions universitaires.
31. National institute of Standards and Technology (NIST), “Face Recognition Vendor Test (FRVT), Part 2: Identification”, NISTIR 8271, septembre 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf (consulté le 6 octobre 2020).
32. National institute of Standards and Technology (NIST), “Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects”, NISTIR 8280, décembre 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (consulté le 6 octobre 2020).
33. Ibid.
34. PR Times, “’Narita Airport Universal Design Basic Plan’ has been decided”, Communiqué de presse, 17 avril 2018, https://prtimes.jp/main/html/rd/p/000000234.000004762.html (consulté le 7 octobre 2020).
35. Comité d’Organisation de Tokyo 2020, “The Tokyo 2020 Accessibility Guidelines”, 24 mars 2017, https://tokyo2020.org/en/organising-committee/accessibility (consulté le 6 octobre 2020).
36. Ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme, “Guidebook on the handling of personal data in One ID services that utilize face recognition technology at airports”, op. cit.
37. Commission européenne, “EU Japan Adequacy Decision”, Fiche d’information, janvier 2019, https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf (consulté le 6 octobre 2020).
38. Organisation internationale de normalisation (ISO), “ISO/IEC 17021-1:2015 Évaluation de la conformité - Exigences pour les organismes procédant à l’audit et à la certification de systèmes de management - Partie 1 : Exigences », iso.org/fr/standard/61651.html (consulté le 7 octobre 2020).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org