



National Security
and Intelligence
Review Agency

Office de surveillance des
activités en matière de sécurité
nationale et de renseignement

ÉTUDE DE L'UTILISATION DE LA BIOMÉTRIE PAR LE GOUVERNEMENT DU CANADA DANS LE CONTINUUM FRONTALIER

OSSNR // Examen 20 - 08

Table des matières

1.	RÉSUMÉ	3
	Liste des acronymes.....	5
	Glossaire.....	8
2.	AUTORITÉS.....	9
3.	INTRODUCTION.....	9
	Renseignements généraux	9
	Étude.....	11
	Portée.....	11
	Critères	12
	Méthodologie et besoins en information	13
	Le rapport	14
4.	PASSÉ DE LA BIOMÉTRIE	14
	Attentats du 11 septembre	15
	Passeport électronique	17
	Programme de biométrie pour les résidents temporaires (PBRT) (2009-2018).....	18
	Par-delà la frontière (2011) et échange de renseignements en matière d'immigration (ERI) (2013-2016)	19
	Projet pilote d'échange d'information entre l'ASFC et IRCC/CIC (2013-2016)	20
	Recherche sur la reconnaissance faciale	21
	Projet pilote et recherche sur l'évaluation opérationnelle par vidéo de l'infrastructure et de la technologie : Reconnaissance faciale par vidéo (PROVE-IT : FRiV) (2011-2013)	22
	Visages en mouvement (FOTM) (2014-2017)	22
	Projet FASTER-PrivBio (2015-2017)	27
	Projet d'expansion de la biométrie (2015-2020).....	29
	Évaluation du <i>passé de la biométrie</i>	30
5.	BIOMÉTRIE ACTUELLE	31
	Programme d'immigration.....	32
	Évaluation du Programme d'immigration	39
	Programme de passeport.....	43
	Évaluation du Programme de passeport	49
	Arrivée au Canada	52
	Bornes d'inspection primaire (BIP).....	52
	NEXUS.....	56

6.	AVENIR DE LA BIOMÉTRIE	57
7.	OBSERVATIONS	66
4.	Projets pilotes.....	70
5.	Évolution des normes juridiques et sociétales.....	71
7.	Systèmes techniques	74
8.	Connaissance des algorithmes	75
9.	Prévention des biais et de la discrimination	76
8.	Conclusion.....	77
Annexe A. Note technique : Systèmes du Programme d’immigration et du Programme de passeport		79
	Programme d’immigration.....	79
	Programme de passeport.....	83
	Responsabilités ministérielles et interconnectivité des systèmes.....	85

1. RÉSUMÉ

Le gouvernement du Canada (GC) a recours à la biométrie pour identifier les personnes avec un degré d'assurance impossible sans les techniques biométriques.

La biométrie joue un rôle fondamental dans le continuum frontalier, notamment pour le contrôle des étrangers cherchant à entrer au Canada et l'identification des voyageurs internationaux dans le mode aérien. Dans la présente étude, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a examiné les activités menées par l'Agence des services frontaliers du Canada (ASFC), Immigration, Réfugiés et Citoyenneté Canada (IRCC) et Transports Canada (TC). Il s'est également intéressé à la Gendarmerie royale du Canada (GRC) qui joue un rôle de soutien dans un des grands programmes d'IRCC dans ce domaine.

Les données biométriques sont des renseignements personnels de nature délicate. L'identification des gens par leurs caractéristiques biologiques soulève des préoccupations au chapitre de la protection de la vie privée et des droits de la personne. La population a des appréhensions au sujet de l'utilisation par le gouvernement de l'analyse biométrique, comme en témoigne le débat sur l'application de la technologie de reconnaissance faciale et, corrélativement, au sujet de l'incidence distincte que cette analyse peut avoir sur les groupes marginalisés. Par ailleurs, l'identification des gens entrant au pays – avec la détermination qui s'ensuit de leur droit d'accéder au territoire canadien ou des risques qui y sont liés –, remplit une fonction de sécurité nationale. Ainsi, l'emploi de la biométrie exige une évaluation du juste milieu à atteindre entre la confidentialité et la sécurité.

Le présent rapport donne un éclairage au débat et le met en contexte; il y contribue en présentant la toute première étude de l'OSSNR sur l'utilisation de la biométrie dans le continuum frontalier.

Celle-ci a permis de formuler un ensemble d'observations liées à neuf thèmes généraux :

1. *Biométrie et sécurité nationale.* Le caractère primordial de l'impératif de sécurité nationale comme justification des activités biométriques a pâli avec le temps au regard d'autres objectifs comme la gestion de l'identité et la facilitation des déplacements des voyageurs. Il devient difficile d'évaluer ces activités *en général* comme relevant de la sécurité nationale. De futures études de l'OSSNR pourraient porter plus précisément sur les activités biométriques directement liées à la sécurité nationale.
2. *Activités établies.* Les activités biométriques établies dans le continuum frontalier sont généralement bien appuyées par les pouvoirs conférés par la loi et conformes à la pratique internationale.
3. *Recours élargi à la biométrie avec le temps.* Le recours à la biométrie dans le continuum frontalier s'est nettement élargi depuis 30 ans et devrait continuer à le faire. Cette trajectoire est tracée à la fois par le perfectionnement des capacités technologiques et l'évolution des défis en matière de gestion de l'identité. Elle est

également présente dans d'autres pays du monde. L'exploitation des possibilités créées par le progrès technologique et le fait de suivre le rythme des autres administrations ne sauraient justifier ce recours accru à la biométrie en soi. Les nouvelles activités dans ce domaine doivent être justifiées par le caractère nécessaire et proportionné d'une collecte et d'une exploitation des données biométriques à des fins particulières voulues.

4. *Projets pilotes.* Les initiatives et les projets pilotes soulèvent plus de préoccupations que les activités établies, risquant d'être entrepris dans un cadre expérimental et sans mesures suffisantes d'analyse juridique ni d'élaboration de politiques. C'est là une question pour laquelle l'intérêt de l'OSSNR ne se dément pas. L'Office s'attend à ce que, faisant abstraction de la nature temporaire ou expérimentale d'un projet, les ministères se livrent à l'analyse nécessaire pour garantir que ses auteurs sont dûment habilités par la loi à mener leur activité et que les tâches connexes de collecte, d'utilisation, de conservation et de communication de renseignements personnels sont bien régies par les politiques.
5. *Évolution des normes juridiques et sociétales.* Le débat public consacré à cette habilitation par la loi est l'occasion de se demander si les normes et les mesures de protection suffisent à réglementer les activités biométriques ou s'il y a lieu d'adopter de nouvelles normes et protections. Comparativement à d'autres domaines, la frontière est un espace où une plus grande intrusion est considérée comme raisonnable, mais cette justification n'est pas illimitée et devra être soigneusement dosée à l'avenir.
6. *Double usage de la biométrie.* L'OSSNR a relevé plusieurs cas de double usage possible de l'information biométrique dans les activités qu'il a examiné. Même si elles présentent des avantages manifestes, les nouvelles utilisations de la biométrie doivent être examinées attentivement pour assurer leur caractère raisonnable et proportionné. De plus, tout nouvel usage doit être justifié et sanctionné par la loi. Le principe de la « limitation de la finalité » peut être un moyen de se prémunir contre un double usage injustifié dans le contexte des activités biométriques.
7. *Systèmes techniques.* Il existe un chevauchement important entre les bases de données et les systèmes techniques exploités dans l'ensemble des activités biométriques établies. L'architecture d'ensemble du système (collecte, communication et stockage de données biométriques dans le cadre des activités du gouvernement du Canada dans le continuum frontalier) est complexe sans nécessairement poser un problème pour autant.
8. *Connaissance des algorithmes.* Les ministères et les organismes ont une connaissance limitée du mode de fonctionnement des algorithmes qu'ils mettent au service de l'analyse biométrique. Chaque ministère ou organisme a toutefois bel et bien démontré que des mesures de leur rendement sont connues et éprouvées et que des seuils spéciaux sont utilisés là où c'est approprié.

9. *Prévention des biais et de la discrimination.* IRCC et l'ASFC ont examiné dans des analyses préliminaires comment leurs activités biométriques pouvaient influencer sur les divers groupes, mais sans apparemment avoir toujours mis en œuvre les stratégies d'atténuation possibles. Dans certains contextes, le progrès technologique a aidé à réduire les incidences distinctes sans les éliminer. Il reste du travail à faire pour atténuer ces effets distincts sur des groupes de la population. Par ailleurs, les ministères et organismes auxquels nous nous sommes intéressés ont démontré qu'ils sont conscients des possibles inégalités systémiques et s'engagent à les combattre.

Ces observations visent à aider les Canadiens à comprendre l'utilisation complexe et évolutive de la biométrie dans le continuum frontalier et dicteront la façon dont l'OSSNR, en tant qu'organisme, orientera ses futurs travaux dans ce domaine.

Le débat public sur l'utilisation que fait le gouvernement de la technologie biométrique continuera d'évoluer, dictant les changements à apporter aux cadres législatif et réglementaire applicables. Un constant examen s'impose en soi de la part de l'OSSNR, plus particulièrement là où la collecte et l'exploitation de données biométriques se justifient par l'évocation expresse des résultats qu'elles permettent d'obtenir sur le plan de la sécurité nationale.

Liste des acronymes

ACS+ – analyse comparative entre les sexes plus

AM – autres ministères

APM – Avis de projet de marché

ASF – agent des services frontaliers

ASFC – Agence des services frontaliers du Canada

AVE – autorisation de voyage électronique

BIP – borne d'inspection primaire

BBGI – Bureau de la biométrie et de la gestion de l'identité

CBP – US Customs and Border Protection

CdC – Chaîne de confiance

CIC – Citoyenneté et Immigration Canada

CIPC – Centre d'information de la police canadienne

COSMOS – Système de gestion des opérations consulaires

CPVPC – Commissariat à la protection de la vie privée du Canada

CRDV – Centre de réception des demandes de visa

CST – Centre de la sécurité des télécommunications Canada

DGDPT – Direction générale du dirigeant principal de la transformation

DLEE – dispositif de lecture électronique des empreintes digitales

DPC – Décret sur les passeports canadiens

DTB – Direction de la transformation de la biométrie

DVN – document de voyage numérique

EFVP – évaluation des facteurs relatifs à la vie privée

ERI – échange de renseignements sur l’immigration

EURODAC – base de données européenne sur la dactyloscopie pour les demandes d’asile

FC – fichier central

FEM – Forum économique mondial

FOTM – Visages en mouvement

GC – gouvernement du Canada

GIJP – Gestion de l’information sur la justice pénale

GRC – Gendarmerie royale du Canada

GTNT – Groupe de travail sur les nouvelles technologies

IATA – Association du transport aérien international

ICP – Infrastructure à clé publique

IIPV – Information interactive préalable sur les voyageurs

IMPP – Initiative de modernisation du Programme de passeport

INTERPOL – Organisation internationale de police criminelle

INVC – Identité numérique des voyageurs connus

IRCC – Immigration, Réfugiés et Citoyenneté Canada

IRIS – Système intégré de récupération d’information

LCISC – *Loi sur la communication d’information ayant trait à la sécurité du Canada*

PFVFT – prise du photo du visage à la frontière terrestre

LIPR – *Loi sur l’immigration et la protection des réfugiés*

LS – liste des signalements

M5 – Groupe des cinq pour les migrations

MJ – ministère de la Justice

NCIC – National Crime Information Center

NIST – National Institute of Standards and Technology

OACI – Organisation de l’aviation civile internationale

BBGI – Bureau de la biométrie et de la gestion de l’identité

OSSNR – Office de surveillance des activités en matière de sécurité nationale et de renseignement

PBRT – Programme de biométrie pour les résidents temporaires

PDE – point d’entrée

PEB – Projet d’expansion de la biométrie

PFVFT – prise du photo du visage à la frontière terrestre

PMP – programme de gestion des passeports

PROVE-IT:FRIV – projet pilote et recherche sur l’évaluation opérationnelle par vidéo de l’infrastructure et de la technologie : Reconnaissance faciale par vidéo

PSN – Politique de sécurité nationale

RDDC – Recherche et développement pour la défense Canada

RIPR – *Règlement sur l’immigration et la protection des réfugiés*

SAID – Système automatisé d’identification dactyloscopique

SCIBI – Système canadien d’identification biométrique aux fins d’immigration

SIAF – Système d’interdiction et d’alerte à la frontière

SIED – Système intégré d’exécution des douanes

SITR – Système d’identification en temps réel

SLTD – Base de données SLTD (documents de voyage et d’identité)

SMGC – Système mondial de gestion des cas

SRF – Solution de reconnaissance faciale

SSOBL – Système de soutien des opérations des bureaux locaux

TBID – base de données sur les identificateurs biométriques des voyageurs

TC – Transports Canada

TUSCAN – Tipoff US-Canada

VSED – vérification systématique des empreintes digitales

Glossaire

Algorithme. Ensemble de règles ou de calculs appliqués aux données qui donnent un résultat interprétable ou déclarable.

Automatisation et prise de décisions automatisée. La prise de décisions automatisée est le processus qui consiste à prendre une décision par des moyens automatisés sans intervention humaine.

Biométrie. Mesure et analyse de caractéristiques biologiques comme les empreintes digitales, les motifs des iris et des rétines, l'ADN et la géométrie de la main et du visage ainsi que l'analyse de certains traits comportementaux comme l'inflexion de la voix, la démarche ou la vitesse de frappe au clavier.

Faux négatif. Incapacité d'établir une correspondance avec l'information biométrique liée à une personne fichée lors de l'interrogation d'un système de données biométriques.

Faux positif. Correspondance erronée avec l'information biométrique d'une personne fichée lors de l'interrogation du système de données biométriques.

Gestion de l'identité. Ensemble de principes, de pratiques, de politiques, de processus et de procédures permettant de réaliser le mandat et les objectifs d'un organisme en matière d'identité.

Identification collective. Processus par lequel une interrogation des données biométriques pour une personne fichée est comparée à des données biométriques de référence de plusieurs personnes fichées en vue de l'obtention d'un ensemble de résultats comparatifs.

Information biométrique. Dossiers de données biométriques ou enregistrements de ces données sous forme d'un ou plusieurs spécimens biométriques à tout stade de traitement.

Inscription. Création et stockage d'un dossier de données attribué à une personne visée par des données biométriques et contenant des données non biométriques avec un ou plusieurs spécimens ou modèles biométriques attribués à un sujet et servant à une comparaison en biométrie.

Modèle biométrique. Ensemble de caractéristiques biométriques stockées et directement comparables servant à prouver des caractéristiques biométriques.

Personne fichée. Personne dont les données biométriques individuelles se trouvent dans le système biométrique.

Interrogation de données biométriques. Spécimen ou caractéristique biométrique fourni à un algorithme à des fins de comparaison biométrique avec une ou plusieurs données biométriques de référence.

Reconnaissance faciale. Reconnaissance automatisée des personnes en fonction des traits du visage.

Vérification individuelle. Processus par lequel une interrogation des données biométriques est comparée à des données biométriques de référence d'une personne fichée à des fins de comparaison.

2. AUTORITÉS

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a réalisé cette étude en vertu de l'alinéa 8 (1) b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*.

3. INTRODUCTION

Renseignements généraux

1. La biométrie permet au gouvernement de mieux savoir qui vous êtes. La mesure et l'analyse des traits biologiques qui vous sont propres, à savoir les empreintes digitales, les motifs des iris, les traits du visage, etc., facilitent l'identification des gens avec un degré d'assurance impossible sans les l'utilisation des techniques biométriques. Il est possible d'utiliser les identificateurs classiques – nom, date et lieu de naissance, sexe, etc. – parallèlement à la biométrie, ce qui améliore le processus d'identification du gouvernement.
2. Savoir qui vous êtes et vérifier que vous êtes bien qui vous prétendez être présente des avantages pour la sécurité nationale. À la frontière, en particulier, les questions posées sur l'identité sont primordiales, déterminant qui a le droit ou non d'entrer au pays et qui pourrait constituer une menace pour la sécurité du Canada et des Canadiens.
3. Par ailleurs, l'identification par les caractéristiques biologiques soulève d'importantes préoccupations en matière de protection de la vie privée et des droits de la personne. Les

données biométriques sont une information foncièrement personnelle et largement immuable (ne pouvant être facilement changée comme peuvent l'être les mots de passe et autres éléments d'identification). Le public a des appréhensions au sujet du recours par le gouvernement à l'analyse biométrique, comme en témoigne les discussions sur l'utilisation de la technologie de reconnaissance faciale et, corrélativement, sur l'incidence distincte qu'elle peut avoir sur les groupes marginalisés¹. Comme la technologie biométrique est de plus en plus présente dans les lieux publics, Il sera important, pour le gouvernement et les Canadiens, de trouver un juste milieu entre les impératifs de sécurité et de protection de la vie privée et les droits de la personne.

4. Notre rapport éclaire et contextualise le débat et y contribue en présentant une étude de fond de l'OSSNR sur l'utilisation de la biométrie par le gouvernement du Canada (GC) dans le continuum frontalier² et en mettant l'accent sur les activités liées au contrôle des étrangers qui cherchent à être admis au Canada et à l'identification des voyageurs du transport aérien international³. L'objectif immédiat de l'étude était de cartographier les activités biométriques dans ce domaine. Cela comprend l'examen de la collecte, de la conservation, de l'utilisation et de la communication de renseignements biométriques, ainsi que des pouvoirs conférés par la loi qui sont à la base de ces activités. La condition de base pour un débat public éclairé est une information fidèle sur les activités menées par le GC et sur la question de savoir si celles-ci sont autorisées par la loi et comment elles le sont.
5. Dans notre étude, nous nous sommes également penchés sur le caractère raisonnable et nécessaire de ces mêmes activités en examinant la précision et la fiabilité de la biométrie avec la possibilité d'une discrimination en fonction de facteurs de distinction comme la race et le sexe. Nous avons considéré le caractère proportionné de la collecte, de la conservation, de l'utilisation et de la communication des données biométriques en question et la transparence avec laquelle le GC parle du recours à la biométrie et de sa contribution à la sécurité nationale.

¹ Tamir Israel, « Facial Recognition at a Crossroads: Transformation at Our Borders and Beyond », Ottawa, CIPPIC, septembre 2020. Consultation le 13 août 2021. https://cippic.ca/uploads/FR_Transforming_Borders.pdf; Petra Molnar, « Technological Testing Grounds: Migration Management Experiment and Reflections from the Ground Up », EDRI/Refugee Law Lab, 2020. Consultation le 13 août 2021. <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>; Hilary Beaumont, « When Border Security Crosses a Line », *The Walrus*, mars-avril 2020. Consultation le 13 août 2021. <https://thewalrus.ca/when-border-security-crosses-a-line/>.

² Le terme « continuum frontalier » est utilisé pour désigner les activités et les processus associés au mouvement international des personnes, y compris les étrangers qui s'installent au Canada (candidats à l'immigration, réfugiés et demandeurs d'asile) et les citoyens canadiens et les résidents permanents qui se déplacent à l'étranger avec des documents de voyage émis par le Canada (p. ex. : des passeports).

³ Par conséquent, notre analyse ne s'est pas étendue aux questions d'application de la législation frontalière à l'intérieur du pays, même si nous notons l'utilisation de logiciels de reconnaissance vocale par l'ASFC dans ce contexte. Au lieu de se présenter à un bureau intérieur de l'ASFC, quelqu'un peut choisir de faire enregistrer sa voix et de la faire vérifier au téléphone par reconnaissance vocale. Les données GPS permettent ensuite de confirmer le lieu où se trouve l'intéressé et donc le respect des exigences d'immigration applicables. Information de l'ASFC à l'OSSNR, 22 octobre 2020.

6. La capacité de l'OSSNR d'examiner l'ensemble des des ministères et organismes et de formuler à la fois des observations particulières et générales – de manière à examiner les arbres autant que la forêt – l'a bien servi au moment d'évaluer le vaste monde de la biométrie en croissance.
7. En plus d'alimenter un important débat public, le rapport qui traite largement le sujet des activités biométriques dans le continuum frontalier s'inscrit dans la mission de l'OSSNR de deux façons. Il délimite d'abord plusieurs domaines plus étroits d'intérêt ou d'inquiétude que l'OSSNR pourrait examiner dans de futures études ciblées. Il définit ensuite un ensemble de critères par lesquels l'Office pourrait évaluer l'usage que fait le GC de la biométrie dans les activités de sécurité nationale et de renseignement à l'intérieur comme à l'extérieur du continuum frontalier.

Étude

Portée

8. La frontière n'est pas comme les autres lieux publics. Des impératifs de sécurité entrent en jeu lorsque des gens franchissent des frontières souveraines, à telle enseigne que l'État est justifié de prendre des mesures qui ne seraient pas permises dans d'autres contextes⁴. Les droits à la vie privée et les libertés civiles ne disparaissent pas, mais les attentes en matière de confidentialité et de liberté de mouvement sont bien moindres. Dans notre examen des activités biométriques du gouvernement du Canada, il était donc pratique de distinguer le continuum frontalier des autres cadres, car ce qui pourrait être trop intrusif dans ces cadres pourrait se justifier dans le cas de la frontière. De plus, la frontière peut servir de banc d'essai à de nouvelles techniques ou technologies biométriques avant que celles-ci ne soient appliquées ailleurs⁵. Compte tenu des préoccupations plus générales en matière de technologie biométrique, la frontière peut être annonciatrice de ce que réserve l'avenir et devrait être examinée en conséquence.
9. Dans cette étude, nous examinons la collecte, la conservation, l'utilisation et la communication de l'information biométrique et évaluons, s'il y a lieu, ces activités au regard des critères que nous allons exposer. Nous avons passé en revue les cadres applicables de politique et de droit qui nous ont été communiqués par les ministères et organismes afin d'éclairer notre évaluation du caractère raisonnable et nécessaire des activités et de jeter les bases d'une connaissance qui orientera les futurs bilans de conformité dans le monde biométrique. Nous avons porté un jugement général sur ce caractère raisonnable et nécessaire, reflétant les thèmes, les tendances et les enjeux qui ressortent de l'examen de l'ensemble des activités biométriques du

⁴ Pour un examen des raisons pour lesquelles la frontière est distincte dans la jurisprudence, voir les paragraphes 22 à 28 de l'arrêt R. c. Simmons, 1988 CanLII 12 (CSC), [1988] 2 RCS 495. Consultation le 18 août 2021. <https://www.canlii.org/fr/ca/csc/doc/1988/1988canlii12/1988canlii12.html>.

⁵ Voir Molnar, « Technological Testing Grounds ».

gouvernement du Canada dans le continuum frontalier. Nous n'avons pas fait de vérification ou d'audit indépendant des affirmations présentées ni des activités mêmes.

10. Dans cette étude, l'OSSNR s'est penché sur les activités de l'Agence des services frontaliers du Canada (ASFC), d'Immigration, Réfugiés et Citoyenneté Canada (IRCC) et de Transports Canada (TC). Il a étendu son analyse à la Gendarmerie royale du Canada (GRC), qui joue un rôle de soutien dans un des grands programmes du continuum frontalier sous la direction d'IRCC.
11. L'OSSNR s'est aussi attardé au passé et à l'avenir possible des activités biométriques dans le continuum frontalier. Le panorama biométrique n'a rien de statique, pas plus que les pratiques de facilitation des mouvements des voyageurs et de sécurisation de la frontière. Les préoccupations de la population en matière de biométrie (et en particulier pour un aspect comme la technologie de reconnaissance faciale) sont surtout liées à ce qui se profile déjà à l'horizon, plutôt qu'aux seules activités en cours. Ainsi, l'analyse des activités, des programmes et des projets pilotes du passé illustre les progrès de la biométrie qui ont mené au moment présent. De même, un certain nombre de projets pilotes et d'initiatives que l'on sait en voie d'élaboration serviront d'exemples de ce qui pourrait être l'avenir. Ce regard plus large contextualise les activités d'aujourd'hui et aide, par conséquent, à atteindre les objectifs plus vastes de notre étude.

Critères

12. Un ensemble de critères de base a guidé l'OSSNR dans l'évaluation des activités biométriques qu'exerce actuellement le gouvernement du Canada dans le continuum frontalier :
 - *Conformité.* L'OSSNR s'est penché sur l'encadrement par les lois et les politiques de la collecte et de l'utilisation de données biométriques par les ministères et les organismes. Il a déterminé si les lois habilitantes respectaient la *Charte canadienne des droits et libertés* et la *Loi sur la protection des renseignements personnels*. Il a aussi examiné les dispositions et les garanties de protection des lois et règlements habilitants de ces mêmes ministères et organismes applicables aux programmes biométriques. Il a enfin examiné les politiques pertinentes des ministères et du Conseil du Trésor.
 - *Proportionnalité.* Dans ce contexte, la proportionnalité s'entend de l'évaluation des objectifs du gouvernement dans son recours à la biométrie par rapport aux conséquences sur la protection de la vie privée ou les droits de la personne. D'une manière générale, l'OSSNR s'attend à ce que toute atteinte aux droits et libertés des individus se justifie d'emblée et offre des avantages de taille dans la réalisation d'objectifs urgents et substantiels.
 - *Fidélité.* Comme la biométrie sert principalement à l'identification des personnes, il importe qu'elle permette de la faire fidèlement de manière à pouvoir contribuer efficacement à la réalisation des objectifs du gouvernement dans une activité ou un programme donné. L'analyse biométrique (avec l'application d'algorithmes) peut être entachée d'erreurs et de fausses correspondances aux importantes conséquences sur les gens. Dans le même ordre

d'idées, les algorithmes d'analyse biométrique peuvent subir l'influence de variables démographiques susceptibles d'engendrer des biais ou de la discrimination.

- *Transparence.* Avec ce critère, l'OSSNR a évalué de façon générale la transparence publique des activités biométriques dans le continuum frontalier à la lumière de l'Engagement de transparence en matière de sécurité nationale pris en 2017 par le gouvernement du Canada. L'accent est mis sur la disponibilité de renseignements sur la nature des données biométriques recueillies et le rapport entre la biométrie et les priorités du GC, notamment en matière de sécurité nationale.
 - *Sécurité des données.* Vu le caractère sensible de l'information biométrique, la protection des données personnelles tout au long de leur cycle de vie (collecte, stockage, communication et destruction) est particulièrement importante. C'est pourquoi l'OSSNR a évalué les politiques-cadres des activités en question sous l'angle des mesures de protection en sécurité des données, qu'il s'agisse du chiffrement, des restrictions d'accès ou des principes de « protection de la vie privée dès la conception ».
13. Collectivement, ces critères ont orienté le jugement porté par l'OSSNR sur le caractère légitime, raisonnable et nécessaire de l'exercice des pouvoirs ministériels en ce qui concerne le recours à la biométrie dans le continuum frontalier canadien. Nos observations mettent en lumière des problèmes et des sujets d'inquiétude sur lesquels un examen approfondi d'activités particulières pourrait se fonder.

Méthodologie et besoins en information

14. L'OSSNR a reçu des renseignements des ministères et organismes sous forme de notes d'information, de réponses écrites et autres documents, dont des énoncés de politique, des guides de procédures, des rapports de projet, des études techniques, des bulletins opérationnels, des manuels, des pièces de correspondance, des sites Web et des avis juridiques pertinents.
15. Il n'y a pas eu que l'information obtenue des ministères et organismes, puisque l'étude, par sa nature même faisant appel à une vaste catégorie de renseignements largement utilisés et analysés dans le monde, justifiait une recherche volumineuse dans des sources ouvertes. L'OSSNR a donc examiné des rapports des médias (tant nationaux qu'internationaux), de l'industrie et des groupes de réflexion, des recherches universitaires, des rapports du gouvernement, des documents d'autres administrations et des études consacrées par des instances intergouvernementales et des organisations non gouvernementales à la biométrie et à sa technologie. Ces recherches ont permis de constater le caractère commun des normes, des thèmes, des risques et même du vocabulaire de la biométrie, autant d'éléments qui ont éclairé nos observations sur les activités biométriques du GC dans le continuum frontalier.

Le rapport

16. Le corps du rapport est divisé en trois parties descriptives présentée dans l'ordre chronologique :
- *passé de la biométrie* : examen de l'histoire et de l'évolution du recours à la biométrie dans le continuum frontalier avec notamment un rappel des projets pilotes d'intérêt et des progrès éminents dans ce domaine;
 - *présent de la biométrie* : description des activités biométriques établies actuelles;
 - *avenir de la biométrie* : examen du rôle que jouera probablement la biométrie dans le continuum frontalier de demain, à en juger par les trajectoires d'aujourd'hui.
17. La dernière section récapitule les thèmes et les observations générales par rapport aux objectifs de l'étude susmentionnés. Certaines observations se rapportent à un programme ou à une activité en particulier, mais d'autres sont valables pour les divers aspects de l'étude. Ce mélange reflète à la fois la nature d'une étude de fond et le mandat transversal unique qui est celui de l'OSSNR. Nos observations vise à permettre aux Canadiens de mieux comprendre l'utilisation complexe et en mutation de la biométrie dans le continuum frontalier et à préciser comment l'OSSNR en tant qu'organisme mènera ses futurs travaux dans ce domaine.

4. PASSÉ DE LA BIOMÉTRIE

18. IRCC a commencé à prendre les empreintes digitales des demandeurs d'asile et des personnes expulsées en 1993⁶, en partie à la suite de la hausse des migrations dans le monde après la fin de la Guerre froide. En 1992, le Canada a reçu 37 000 demandes d'asile comparativement aux quelques milliers qu'il recevait annuellement dans les années 1980⁷. Les pressions que cela a exercé sur le système sont une des raisons derrière le dépôt du projet de loi C-86 en juin 1992. Celui-ci comportait plusieurs dispositions visant à accroître l'efficacité et l'intégrité du système canadien d'immigration et d'asile avec, entre autres mesures, la prise des empreintes digitales des demandeurs d'asile et des personnes expulsées⁸. Cette dernière disposition a suscité les critiques du public et le gouvernement l'a modifiée en prévoyant la suppression des empreintes

⁶ IRCC, « Évaluation de l'initiative de biométrie (état stable) et de l'initiative d'échange de renseignements en matière d'immigration (ERI) entre le Canada et les États-Unis », octobre 2019, p. 1 [OSSNR_202002_005, p. 1].

⁷ Ninette Kelley et Michael J. Trebilcock, *The Making of the Mosaic: A History of Canadian Immigration Policy*. (Toronto : Toronto University Press, 2010), p. 381.

⁸ Valerie Knowles, *Strangers at Our Gates: Canadian Immigration and Immigration Policy, 1540-2015*. (Toronto : Dundurn Press, 2016), p. 239. Des considérations en matière de sécurité nationale entraient également en jeu dans le cas de ce projet de loi. Pour une analyse, voir Sharryn J. Aiken, « Of Gods and Monsters : National Security and Canadian Refugee Policy », *Revue québécoise de droit international*, 2001. 14 (2). Consultation le 19 août 2021. <https://www.sqdi.org/wp-content/uploads/14.2 - aiken.pdf>.

digitales au moment de l'accession à la citoyenneté canadienne⁹. En fin de compte, le but de la collecte de données dactyloscopiques était d'améliorer l'efficacité du traitement dans le système tant par une meilleure détection que par la dissuasion des fraudes grâce à une gestion rigoureuse de l'identité¹⁰.

19. Dans les années qui ont suivi, la collecte et l'utilisation de données biométriques dans le continuum frontalier se sont constamment étendues, si bien que presque tous les gens qui arrivaient au Canada par avion – qu'il s'agisse d'étrangers ou de citoyens canadiens – voyaient dès lors leurs données biométriques être recueillies et/ou analysées de quelque manière. Comment ce cheminement s'est-il fait? Nous répondrons à cette question ici en décrivant l'évolution dans le temps des activités du gouvernement du Canada et en mettant en évidence les moments, les programmes et les projets clés dont cette évolution a été jalonnée.

Attentats du 11 septembre

20. Les attentats terroristes du 11 septembre 2001 ont transformé considérablement le panorama de la sécurité nationale au Canada. Le budget de 2001 s'est fait le reflet des nouvelles priorités du jour, affectant 7,7 milliards sur cinq ans aux mesures de sécurité, dont 1 milliard au contrôle et à l'exécution de la loi en matière d'immigration et 1,2 milliard aux initiatives de sécurisation de la frontière¹¹.
21. Ces dépenses suivaient de près les recommandations expresses d'un comité parlementaire cherchant, entre autres, à « moderniser la gestion de la frontière afin de satisfaire aux besoins futurs en matière de sécurité et de commerce » et à faire en sorte que « le gouvernement du Canada essaie des technologies de pointe et qu'il en dote ses services frontaliers »¹². Cette dernière recommandation s'accompagnait d'une suggestion : « la technologie biométrique, soit l'analyse des empreintes digitales ou de la rétine, pourrait aussi être envisagée pour identifier les particuliers et les camionneurs qui traversent la frontière¹³ ». Le document demandait également que soit remis en service et entièrement mis en œuvre le programme NEXUS, projet pilote sur les voyages transfrontaliers États-Unis-Canada qui avait été lancé en novembre 2000, mais suspendu à la suite des attentats.

⁹ *Strangers at Our Gates*, p. 240.

¹⁰ *Strangers at Our Gates*, p. 239. Ainsi, quelqu'un ne pouvait pas présenter plusieurs demandes sous plusieurs noms, ni présenter à nouveau une demande déjà rejetée sous un nom différent.

¹¹ Ministère des Finances Canada, *Le plan budgétaire de 2001 : Comprendre les renseignements supplémentaires et les Avis de motions de voies et moyens*, Ottawa, 2001. Consultation le 1^{er} septembre 2021.

<https://www.budget.gc.ca/pdfarch/budget01/pdf/bpf.pdf>.

¹² Chambre des communes, *Vers une frontière sûre et propice à l'efficacité commerciale : rapport du Comité permanent des affaires étrangères et du commerce international*, p. xi-x. Consultation le 1^{er} septembre 2021.

<https://www.noscommunes.ca/DocumentViewer/fr/37-1/FAIT/rapport-13>.

¹³ Chambre des communes, *Vers une frontière sûre et propice à l'efficacité commerciale*, p. 17.

22. La pièce maîtresse de la coopération canado-américaine en matière de sécurité frontalière a cependant été la *Déclaration sur la frontière intelligente* signée le 12 décembre 2001. Accompagnée d'un plan d'action en 30 points, cette déclaration devait guider les États-Unis et le Canada dans leurs efforts de sécurisation de la frontière. La toute première mesure dans ce plan d'action est l'introduction d'« identificateurs biométriques », les deux pays étant appelés à [traduction] « mettre au point en toute urgence des identificateurs biométriques communs dans des documents comme les cartes de résident permanent, les cartes NEXUS et d'autres documents de voyage pour une plus grande sécurité¹⁴ ». À noter également les dispositions visant à élargir l'échange de renseignements dans le contexte des demandes de visa, d'asile et de réinstallation de réfugiés¹⁵.
23. Les deux pays ont expressément formulé le *Plan d'action sur la frontière intelligente* comme un effort en vue de [traduction] « créer une zone de confiance contre les activités terroristes¹⁶ ». Aux États-Unis, le rapport final de la National Commission on Terrorist Attacks Upon the United States (mieux connu sous le nom de « Rapport de la Commission sur le 11 septembre ») a exprimé cette logique appelant à l'instauration d'un [traduction] « système de contrôle biométrique » embrassant tout le continuum frontalier de la demande de passeport ou la demande d'immigration à l'arrivée au point d'entrée, en passant par l'échange de renseignements entre les administrations¹⁷. De même, la *Politique de sécurité nationale* (PSN) de 2004 du Canada a mis la biométrie au premier plan dans son chapitre sur la sécurité frontalière¹⁸. La PSN dit que le Canada « veillera à étendre le recours à la biométrie » et « étudiera des façons de recourir à la biométrie dans les systèmes touchant la frontière et l'immigration afin d'améliorer les processus de conception et de délivrance de documents de voyage et de preuve de statut, et de valider l'identité des voyageurs aux points d'entrée »¹⁹. Aux yeux des deux pays, la biométrie est un moyen de repérer les terroristes qui peuvent traverser la frontière. Les événements du 11 septembre ont eu pour effet d'associer sécurité frontalière et sécurité nationale et d'ériger la gestion de l'identité – jusque-là surtout liée aux questions d'efficacité et de fraude – en une priorité de sécurité nationale.

¹⁴ Legislation Online, « U.S. and Canada Smart Border Declaration (2001) ». Consultation le 1^{er} septembre 2021.

<https://www.legislationonline.org/documents/id/7543>.

¹⁵ Legislation Online, « U.S. and Canada Smart Border ».

¹⁶ Office of Homeland Security, « Action Plan for Creating a Secure and Smart Border », 12 décembre 2001. Consultation le 13 septembre 2021. <https://georgewbush-whitehouse.archives.gov/news/releases/2001/12/20011212-6.html>.

¹⁷ National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Washington, 2004. Consultation le 1^{er} septembre 2021. <http://govinfo.library.unt.edu/911/report/911Report.pdf>. Ce rapport formule aussi un important changement dans la vision de ces questions en faisant remarquer ce qui suit : [traduction] « [D]ans la décennie qui a précédé le 11 septembre 2001, la sécurité de la frontière, ce qui comprend les voyages, les entrées et l'immigration, n'était pas considérée comme une question de sécurité nationale, [mais à la suite des attentats] les documents de voyage sont [devenus] aussi importants que les armes. Les terroristes doivent voyager clandestinement pour se rencontrer, s'entraîner, planifier, cadrer leurs cibles et passer à l'attaque » (p. 383 et 384).

¹⁸ Bureau du Conseil privé, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Ottawa, avril 2004, p. 50. Consultation le 19 juillet 2021. <https://securitepublique.gc.ca/cnt/ntnl-scrnt/scrng-fr.aspx>.

¹⁹ Bureau du Conseil privé, *Protéger une société ouverte*, p. 50.

24. Au Canada, la PSN établit le canevas des activités biométriques établies actuelles du gouvernement du Canada, soit la reconnaissance faciale dans la délivrance et l'utilisation des documents de voyage (Programme de passeport) et la prise des empreintes digitales, d'une part, et la validation de l'identité aux points d'entrée (Programme d'immigration), d'autre part. Nous y reviendrons à la section V.
25. Dans le reste de cette section, nous décrivons brièvement les grands programmes et activités biométriques adoptés dans les années qui ont suivi les attentats du 11 septembre.

Passeport électronique

26. Bien qu'elle soit la norme pour le passeport depuis des décennies, la photo n'était pas considérée comme de la « biométrie » tant que le passeport n'a pas été lisible par machine. Les lignes directrices de 2003 de l'Organisation de l'aviation civile internationale (OACI) sur les passeports électroniques, communément appelés « passeports biométriques », ont ainsi marqué l'introduction des identificateurs biométriques dans ce document sur la scène internationale. Le Canada a opté pour le passeport électronique en 2004, mais sa mise en œuvre a ensuite eu lieu par étapes et ce n'est qu'en 2013 qu'il a été pleinement fonctionnel. Des centaines d'autres administrations ont adopté le passeport électronique au cours de cette période²⁰, en faisant progressivement une pratique internationale recommandée pour les documents de voyage officiels. Il sera question de la présente version de ce passeport aux paragraphes 95 à 112 plus loin.
27. En plus de la « puce intelligente » intégrée au passeport électronique et contenant l'image faciale, le Canada a adopté la reconnaissance faciale dans le cadre de la demande et de la délivrance de passeports. La première évaluation des facteurs relatifs à la vie privée (EFVP) pour ce qui était alors connu sous le nom de « projet de reconnaissance faciale » a été effectuée en 2003, mais la pleine réalisation de ce projet sous le nom de « solution de reconnaissance faciale » (SRF) n'a pas eu lieu avant 2010. Le système recourait à la reconnaissance faciale pour mieux évaluer le droit à un passeport ou à un autre document de voyage canadien²¹. Le programme visait expressément à détecter la fraude, à appuyer la vérification de l'identité et à prévenir la délivrance de passeports à des demandeurs inadmissibles²². Nous abordons aux paragraphes 95 à 112 la version actuelle de la SRF comme pièce maîtresse du Programme de passeport dans sa mouture actuelle.

²⁰ Dans le monde, 60 % des passeports délivrés en 2009 étaient électroniques. En 2013, au moins une centaine de pays avaient adopté une version électronique du document. Voir gouvernement du Canada, « L'histoire du passeport électronique canadien », 13 mai 2014. Consultation le 1^{er} septembre 2021.

<https://www.canada.ca/fr/nouvelles/archive/2014/05/histoire-passeport-electronique-canadien.html>.

²¹ Par exemple, certificats d'identité ou documents de voyage pour réfugiés dans le cas des non-Canadiens.

²² Passeport Canada, « PIA Facial Recognition Project 2011 », p. ii. [IRCC DR n° 2 Documents].

Programme de biométrie pour les résidents temporaires (PBRT) (2009-2018)

28. Lancé en 2009²³ et mis en service en 2013, le « Programme de biométrie pour les résidents temporaires » (PBRT) a constitué un grand pas en avant dans la collecte de données biométriques aux fins de l'immigration. Dans ce programme, IRCC (alors appelé Citoyenneté et Immigration Canada ou CIC) recueillait des données biométriques (empreintes digitales et photo numérique) dans le cadre des demandes de résidence temporaire²⁴ présentées par des ressortissants de 30 nationalités²⁵. Les empreintes digitales étaient contrôlées [traduction] « par rapport à des fiches dactyloscopiques détenues par le gouvernement du Canada sur les criminels connus, les ex-demandeurs d'asile, les personnes déjà expulsées et les anciens candidats à l'immigration²⁶ ». Une fois la demande approuvée et le demandeur arrivé au pays, l'ASFC vérifiait²⁷ les données biométriques pour s'assurer que la personne qui se présentait était bien celle qui avait fait la demande. En 2014, la collecte de données biométriques s'est étendue des demandes de résidence temporaire aux demandes d'asile et de réinstallation de ressortissants étrangers²⁸.

²³ Dans le budget de 2008, 26 millions de dollars ont été affectés sur deux ans au projet, l'intention étant d'« accroître l'intégrité et l'efficacité de la frontière en empêchant les criminels d'entrer au Canada et en rendant la procédure plus simple pour les personnes qui sont en règle ». Ministère des Finances Canada, « Budget de 2008 », 26 février 2008. Consultation le 18 août 2021. <https://www.budget.gc.ca/2008/pdf/plan-fra.pdf>, p. 203. Voir aussi Gouvernement du Canada, « Biometrics Expansion Project: Project Charter », Bureau de réalisation de projets, 20 juillet 2018, p. 2 [OSSNR_202002_033, p. 2].

²⁴ Les demandes de résidence temporaire comprennent les demandes de visa de visiteur (de tourisme) et de permis de travail ou d'études.

²⁵ La liste comprenait l'Afghanistan, l'Albanie, l'Algérie, le Bangladesh, la Birmanie (Myanmar), le Cambodge, la Colombie, la République démocratique du Congo, l'Égypte, l'Érythrée, Haïti, l'Iran, l'Irak, la Jamaïque, la Jordanie, le Laos, le Liban, la Libye, le Nigeria, le Pakistan, l'Arabie saoudite, la Somalie, le Soudan du Sud, le Soudan, le Sri Lanka, la Syrie, la Tunisie, le Vietnam, le Yémen et l'Autorité palestinienne. Voir IRCC, « Évaluation de l'initiative de biométrie (établie et de l'initiative d'échange de renseignements en matière d'immigration (ERI) entre le Canada et les États-Unis », p. 35 [OSSNR_202002_005, p. 35].

²⁶ Gouvernement du Canada, « Biometrics Expansion Project: Project Charter », Bureau de réalisation de projets, 20 juillet 2018, p. 2 [OSSNR_202002_033, p. 2].

²⁷ À titre discrétionnaire à certains points d'entrée.

²⁸ ASFC, « Biometrics Expansion Transition », 4 mars 2020, p. 2 [OSSNR_202002_009, p. 2]. D'un point de vue technique, cette expansion ne relevait pas du Programme de biométrie pour les résidents temporaires, qui s'adressait seulement aux demandeurs de résidence temporaire. La collecte de données biométriques dans le cadre des demandes d'asile et de réinstallation de ressortissants étrangers relevait de pouvoirs discrétionnaires distincts. Dans l'ensemble, cependant, la collecte de données biométriques auprès des personnes déportées, des demandeurs d'asile, des demandeurs de résidence temporaire dans le cadre du PBRT et des demandeurs de réinstallation de ressortissants étrangers ou de réfugiés représentait la biométrie établie à l'époque.

29. Selon le gouvernement du Canada, la biométrie a été adoptée comme moyen d'accéder à des renseignements plus complets et exacts de manière à éclairer les décisions prises sur l'admissibilité des demandeurs de résidence temporaire²⁹ en vertu de la *Loi sur l'immigration et la protection des réfugiés* (LIPR)³⁰. Ce recours à la biométrie dans le PBRT appuyait donc la réalisation d'objectifs de gestion de l'identité, la sécurité nationale – et l'identification des gens pouvant présenter une menace pour la sécurité – constituant un élément de soutien du programme.

Par-delà la frontière (2011) et échange de renseignements en matière d'immigration (ERI) (2013-2016)

30. En 2011, le Canada et les États-Unis ont produit la déclaration commune *Par-delà la frontière : Une vision commune de la sécurité du périmètre et de la compétitivité économique* avec son document d'accompagnement « Plan d'action Par-delà la frontière ». Ce plan formulait l'engagement pris par les deux pays d'accroître les échanges de renseignements³¹. Depuis 2003, le Canada et les États-Unis échangeaient des renseignements au cas par cas, c'est-à-dire ponctuellement, mais ce processus était laborieux et donc peu fréquent.
31. Le programme qui en est résulté est l'initiative d'échange de renseignements en matière d'immigration (ERI) qui permettait aux autorités canadiennes et américaines d'échanger systématiquement des renseignements sur l'immigration lors de correspondances biométriques dans leurs bases de données respectives, une capacité qui est devenue pleinement fonctionnelle en août 2015³². Par exemple, au moment de soumettre une demande, tous les demandeurs³³ qui devaient fournir des données biométriques au Canada voyaient leurs empreintes digitales

²⁹ En vertu de la LIPR entrée en vigueur en 2002 et toujours en application, des gens peuvent avoir l'interdiction d'entrer sur un territoire pour des raisons de sécurité (article 34), d'atteinte aux droits humains ou internationaux (article 35), de criminalité (article 36 et 37), de santé (article 38), d'incapacité financière (article 39), de fausses déclarations (article 40), de manquement à la loi (article 41) ou en raison d'un membre de la famille interdit de territoire (article 42).

³⁰ Gouvernement du Canada, « Sommaire de Projet de biométrie pour les résidents temporaires (PBRT) », 27 décembre 2020. Consultation le 21 juillet 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/transparence/acces-information-protection/evaluation-facteurs-relatifs-vie-privee/projet-biometrie-residents-temporaires-2012.html>.

³¹ La Maison-Blanche, « United States-Canada Beyond the Border : A Shared Vision of Perimeter Security and Economic Competitiveness », décembre 2011. Consultation le 21 juillet 2021. <https://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf>, p. iii.

³² IRCC, « Evaluation of the Biometrics (Steady State)... », p. 3 [OSSNR_202002_005, p. 3]; voir aussi Sécurité publique Canada, « Par-delà la frontière – Rapport de mise en œuvre 2015 », 29 septembre 2016. Consultation le 21 juillet 2021. <https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2015-bynd-brdr-mplmntn/index-fr.aspx>. L'initiative ERI comprenait également l'échange de renseignements biographiques.

³³ À l'époque, il s'agissait de demandeurs de résidence temporaire de 30 nationalités dans le cadre du PBRT, ainsi que de demandeurs d'asile et de réinstallation de réfugiés.

systématiquement vérifiées par rapport aux données dactyloscopiques des États-Unis³⁴. En cas de correspondance, les Américains renvoyaient l'information utile en matière d'immigration (renseignements biographiques pour confirmer l'identité, résultat de toute demande antérieure d'immigration, etc.) à IRCC pour éclairer les décisions d'admissibilité. L'entente était réciproque et les États-Unis procédaient à une recherche semblable dans les données dactyloscopiques de l'immigration du Canada avec communication des renseignements en cas de correspondance. Comme le précise un rapport de mise en œuvre de 2015, cette capacité aura permis « de lutter contre la fraude d'identité, de renforcer la gestion de l'identité et de fournir de l'information importante afin d'orienter les décisions de chaque pays en matière d'admissibilité³⁵ ».

32. L'ERI était à maints égards le prolongement naturel du PBRT. Si le PBRT rendait possible le contrôle des données biométriques d'un demandeur par une consultation des bases de données du Canada, l'ERI étendait cette possibilité aux bases de données américaines, élargissant ainsi l'éventail des renseignements pouvant être obtenus par l'interrogation des données biométriques.

Projet pilote d'échange d'information entre l'ASFC et IRCC/CIC (2013-2016)

33. À compter de 2013, un projet pilote en deux étapes réalisé par l'ASFC et IRCC/CIC a permis d'explorer les divers avantages de l'échange d'information concernant la reconnaissance facile. Ce projet avait pour but, à titre d'expérience, d'interroger la base de données des passeports d'IRCC/CIC à l'aide de 72 photos de personnes recherchées par l'ASFC. Cette recherche visait à vérifier si des passeports avaient été délivrés à des gens visés par des mandats d'arrestation de l'ASFC en vertu de la LIPR (sous une fausse ou une vraie identité), et d'ainsi protéger l'intégrité du système des passeports, ce qui devait aussi faciliter l'exécution de la LIPR. L'ASFC et IRCC se fondent sur l'article 7 et les alinéas 8 (2) a) et 8 (2) e) de la *Loi sur la protection des renseignements personnels* pour l'utilisation et la communication de cette information³⁶.

³⁴ Dans le cadre du PBRT, environ 400 000 demandes de renseignements ont été envoyées chaque année. Gouvernement du Canada, « Biometrics Expansion Project: Project Charter », p. 3 [OSSNR_202002_033, p. 3].

³⁵ « Par-delà la frontière – Rapport de mise en œuvre 2015 », 29 septembre 2016. Consultation le 21 juillet 2021. <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/2015-bynd-brdr-mplmntn/index-fr.aspx>.

³⁶ IRCC et ASFC, « Annexe sur l'échange d'information du protocole d'entente entre IRCC et l'ASFC, 2017, p. 156. L'annexe traite des renseignements de l'immigration et des douanes (OSSNR_202004_156, p. 12). La communication de renseignements de l'ASFC à IRCC peut s'appuyer sur l'alinéa 8 (2) a) de la *Loi sur la protection des renseignements personnels* (usages compatibles) et l'article 5 de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* ou, dans le cas de l'information douanière, sur l'alinéa 107 (5) j) de la *Loi sur les douanes* qui autorise l'ASFC à communiquer à IRCC l'information recueillie aux fins de la *Loi sur les douanes* ou du *Tarif des douanes* aux fins de l'administration ou de l'application de la *Loi sur la citoyenneté*, de la LIPR ou de la législation canadienne sur les passeports et autres documents de voyage (voir aussi le paragraphe 5 de l'annexe III). De son côté, IRCC peut s'appuyer sur l'alinéa 8 (2) a) de la *Loi sur la protection des renseignements personnels* (usages compatibles) ou sur l'alinéa 8 (2) e) de la *Loi sur la protection des renseignements personnels* lorsque la communication est destinée à trois services de l'ASFC

34. L'identification collective de ces 72 individus par reconnaissance faciale a permis de découvrir trois personnes qui avaient acquis frauduleusement des documents de voyage. Se fondant sur ces résultats, les organismes ont conclu un protocole d'entente (PE) en décembre 2013 en vue d'échanger les photos d'un millier de personnes recherchées sur mandat en cours de l'ASFC. Ils ont procédé à une identification collective par une recherche de reconnaissance faciale dans la base de données sur les passeports. Cette fois, ils ont relevé 15 personnes ayant fait des demandes frauduleuses de passeport³⁷.
35. En 2015, une autre étape du projet a été lancée en vertu d'un PE ultérieur et le nombre d'individus visés était alors de 3 000. Il y a également eu élargissement de l'information pouvant être communiquée en cas de correspondance. Si le PE de 2013 autorisait seulement l'échange de renseignements relatifs aux fraudes liées aux documents, le PE de 2015 permettait l'échange de tous les renseignements considérés comme préjudiciables³⁸ aux fins de l'exécution de la LIPR³⁹. L'appendice III de l'annexe sur l'échange d'information du protocole d'entente IRCC-ASFC de 2017 a conféré des bases permanentes à cet échange de renseignements⁴⁰.

Recherche sur la reconnaissance faciale

36. En plus de l'expansion, du perfectionnement et de la valorisation des activités biométriques liées aux passeports et à l'immigration, le Canada a aussi exploré d'autres utilisations de la biométrie, notamment la reconnaissance faciale, par la recherche sur les technologies émergentes et au moyen d'initiatives pilotes, mettant à l'essai d'éventuelles applications dans le continuum frontalier.

(Division de l'exécution de la loi dans les bureaux intérieurs, Direction des opérations du renseignement et du ciblage et Division des enquêtes criminelles). Ces services de l'Agence sont désignés comme « organismes d'enquête » admissibles aux fins de l'alinéa 8 (2) e) de l'annexe II du *Règlement sur la protection des renseignements personnels*.

³⁷ ASFC, « CBSA – Citizenship and Immigration Canada Information Exchange on Individuals Wanted Under the Immigration and Refugee Protection Act », sans date

³⁸ Dans ce contexte, les renseignements préjudiciables sont des renseignements qui peuvent indiquer une contravention aux lois applicables.

³⁹ ASFC, « CBSA – Citizenship and Immigration Canada Information Exchange », p. 2 [OSSNR_202002_065, p. 2].

⁴⁰ IRCC et ASFC, Annexe sur l'échange d'information du protocole d'entente IRCC-ASFC [OSSNR_202004_156, p. 12].

Projet pilote et recherche sur l'évaluation opérationnelle par vidéo de l'infrastructure et de la technologie : Reconnaissance faciale par vidéo (PROVE-IT : FRiV) (2011-2013)

37. En 2011, l'ASFC a dirigé⁴¹ le « projet pilote et recherche sur l'évaluation opérationnelle par vidéo de l'infrastructure et de la technologie : Reconnaissance faciale par vidéo » (projet PROVE-IT : FRiV). Il a examiné en laboratoire la possibilité de recourir à la reconnaissance faciale de captures en direct dans un environnement contrôlé comme celui d'un aéroport⁴². Les chercheurs ont regardé les produits et outils commerciaux disponibles à cette fin et ont déterminé que la [traduction] « surveillance faciale » était prête à être utilisée en direct [traduction] « dans des environnements semi-restreints »⁴³.

Visages en mouvement (FOTM) (2014-2017)

38. Fort des constatations et des résultats de PROVE-IT : FRiV, l'ASFC a lancé en 2014 le projet pilote « Visages en mouvement » (FOTM)⁴⁴. Il s'agissait de la capture en direct par vidéo d'images faciales de voyageurs passant par l'aérogare 3 de l'aéroport international Pearson à Toronto pendant une période de six mois de juin à novembre 2016.
39. On avait installé des vidéocaméras expressément pour ce projet en vue de capter des images faciales dans l'aire des arrivées de l'immigration, à l'inspection primaire et vers la sortie après le traitement au primaire⁴⁵. On a contrôlé en temps réel les images à l'aide de la reconnaissance faciale dans deux bases de données d'imagerie, à savoir une liste de surveillance « témoin » comptant 65 bénévoles de l'ASFC et une liste de surveillance « opérationnelle » formée de 4 860 personnes déjà expulsées, produite par l'Agence. Les bénévoles en question ont effectué plus de 1 200 visites d'essai pendant les six mois de cette démonstration.

⁴¹ De concert avec l'École de technologie supérieure (ETS) et avec l'appui de plusieurs partenaires, dont la GRC, Recherche et développement pour la défense Canada (RDDC), Transports Canada, le ministère des Affaires étrangères et du Commerce international (MAECI), le Bureau du Conseil privé (BCP), l'Université d'Ottawa, le FBI (États-Unis), le ministère de l'Intérieur ou Home Office (Royaume-Uni) et le National Institute of Standards and Technology (NIST).

⁴² ASFC, « PROVE-IT : FRiV : Framework and Outcomes », avril 2014. Consultation le 22 juillet 2021.

<https://www.nist.gov/document/14-nist-friv-gorodnichy-ppdf>.

⁴³ Face4 Systems Inc., « Canada Border Services Agency Faces-on-the-Move Demonstration Project : High-Level Architecture », sans date, p. 1 [OSSNR_202002_070, p. 1]. Les résultats du projet PROVE-IT (FRiV) ont été présentés en 2014 à l'occasion de la conférence internationale « Biometrics Performance » parrainée par le National Institute of Standards and Technology (NIST). Voir NIST, « IBPC 2014 Presentations », 5 décembre 2016. Consultation le 22 juillet 2021. <https://www.nist.gov/itl/iad/image-group/ibpc-2014-presentations>.

⁴⁴ Le partenaire industriel aux fins de ce projet était Face4 Systems Inc., une entreprise privée de technologie ayant son siège à Ottawa (Canada). L'École de technologie supérieure (ETS) a assuré la surveillance de la méthodologie et de l'analyse dans ce projet expérimental.

⁴⁵ Face4 Systems Inc., « Face4 Final Report for CSSP Project CSSP – 2014... », p. 25 [OSSNR_202002_072, p. 25].

Parallèlement, de 15 000 à 20 000 voyageurs étaient contrôlés par jour à l'aide de la liste de surveillance opérationnelle. Pour 47 d'entre eux, il y a eu détection par le système⁴⁶. Tous les dossiers de renseignements personnels devaient être détruits à la fin du projet sauf ceux qui ont servi à des fins administratives et qui devaient être conservés pendant deux ans après la date de leur dernière utilisation conformément au paragraphe 6 (1) de la *Loi sur la protection des renseignements personnels* et à l'alinéa 4 (1) a) de son règlement d'application⁴⁷.

40. Le but immédiat avec le projet FOTM était de faire en sorte que la technologie de reconnaissance faciale soit fin prête à être utilisée en direct et en temps réel dans un environnement contrôlé⁴⁸. Un autre objectif était d'établir des protocoles de confidentialité et de sécurité devant régir le déploiement de la technologie de la reconnaissance faciale et l'offre de services de l'industrie canadienne dans ce domaine grâce à une collaboration avec l'ASFC et à un accès au cadre opérationnel de cet organisme (la frontière en l'occurrence). Entre autres objectifs stratégiques à plus long terme, il y avait la promotion d'une [traduction] « circulation efficace des gens à la frontière canadienne » et la prise en charge des [traduction] « menaces en évolution pour la sécurité publique à la frontière ou avant [...] dans le respect des valeurs canadiennes, et notamment du droit à la vie privée⁴⁹ ». À la fin, le FOTM a été présenté comme un élément constitutif des futures applications de la reconnaissance faciale dans le continuum frontalier et [traduction] « des scénarios de sécurité semblables (installations de transport, centres commerciaux, stades, rassemblements de masse)⁵⁰ ». Les leçons tirées du FOTM devaient alimenter en données une [traduction] « feuille de route » de l'utilisation [traduction] « de la science et de la technologie [...] pour la surveillance faciale, en particulier à la frontière »⁵¹.
41. Selon le rapport final, le projet FOTM a fait face à plusieurs défis stratégiques en ce qui concerne [traduction] « notamment le concept d'opération, les contraintes de déploiement, la notification

⁴⁶ Se sont ajoutées 25 décisions erronées pour un taux d'erreur de 0,34 % dans l'ensemble [OSSNR_202002_070, p. 57]. On entend par décision erronée en ligne la confirmation par erreur d'une correspondance avec la liste de surveillance par un opérateur humain en temps réel à l'aéroport. En revanche, les décisions hors ligne étaient portées hors de ce cadre opérationnel et sans que le temps presse. Si le système produisait de multiples faux positifs par jour, il fallait le jugement humain pour confirmer toute correspondance signalée par le système. Les décisions erronées sont donc plus importantes que les faux positifs, ceux-ci étant un produit connu et nécessaire de la technologie applicable (la sensibilité relative du seuil de correspondance engendrera plus ou moins de faux positifs et de faux négatifs) alors que les décisions erronées tiennent à une défaillance réelle de tout le système, notamment de ses opérateurs humains.

⁴⁷ ASFC, « Sommaires des évaluations des facteurs relatifs à la vie privée : Archivé – Filtrage des personnes à surveiller à l'aide de caméras multiples », 22 juillet 2016. Consultation le 23 juillet 2021, <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airpr/fotm-fra.html>; *Loi sur la protection des renseignements personnels*, L.R.C., ch. P-21; *Règlement sur la protection des renseignements personnels*, DORS/83-508.

⁴⁸ Face4 Systems Inc., « Canada Border Services Agency Faces-on-the-Move Demonstration Project : Test Plan », sans date, p. 1 [OSSNR_202002_069, p. 1]; Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014 – CP – 2000, Faces-on-the-Move Multi-Camera Watchlist Screening », 31 mars 2017, p. 12 [OSSNR_202002_072, p. 12].

⁴⁹ Face4 Systems Inc., « Faces-on-the-Move Demonstration Project: Concept of Operations (CONOPS) », sans date, p. 1 [OSSNR_202002_068, p. 1].

⁵⁰ Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014... », p. 11 [OSSNR_202002_072, p. 11].

⁵¹ Face4 Systems Inc., « Faces-on-the-Move Demonstration Project: Test Plan », p. 1 [OSSNR_202002_069, p. 1].

publique, la sécurité des données, les règles de conservation et de purge des données et la légalité des mesures d'exécution compte tenu des problèmes que posent la reconnaissance faciale et la protection des renseignements personnels⁵² ». Ces défis et d'autres étaient susceptibles [traduction] « d'influencer les futurs déploiements de la surveillance faciale et/ou les feuilles de route en matière technologique ». On convenait néanmoins que la combinaison de capacités avancées et d'un adoucissement de la résistance du public à la technologie de la reconnaissance faciale [traduction] « déterminerait le besoin d'investir continuellement tant dans la science que dans l'application de la surveillance par reconnaissance faciale⁵³ ».

42. Avant la période de démonstration, une EFVP portant sur le FOTM effectuée en consultation avec le Commissariat à la protection de la vie privée (CPVP) avait mis d'autres questions en lumière⁵⁴. Il en est résulté certains changements apportés au projet. On a notamment renoncé à utiliser les photos de liste de surveillance de plusieurs organismes gouvernementaux et on a laissé tomber le signalement prévu de la présence d'une personne déjà expulsée aux organismes d'application de la loi si celle-ci n'avait pas été interceptée par l'ASFC avant qu'elle ne quitte le point d'entrée⁵⁵. Dans le rapport final du projet, les experts-conseils [traduction] « convenaient que, si la reconnaissance faciale devait être mise en service dans une perspective à long terme, l'EFVP devrait être refaite et renouvelée en vue de reconnaître les éventuels risques permanents qui n'influaient pas sur le projet FOTM à court terme⁵⁶ ». Qui plus est, l'ASFC reconnaissait que, si le FOTM devait devenir un programme permanent, le recours à la reconnaissance faciale exigerait une mise à jour de la *Politique de l'ASFC sur l'utilisation ouverte de la technologie de surveillance et d'enregistrement audiovisuel* et de la description du fichier connexe de renseignements personnels⁵⁷ (FRP) de l'Agence, soit le PPU 1104, qui ne faisait pas mention de [traduction] « renseignements biométriques⁵⁸ ».

⁵² Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014... », p. 71 [OSSNR_202002_072, p. 71].

⁵³ Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014... », p. 72 [OSSNR_202002_072, p. 72].

⁵⁴ ASFC, « Sommaires des évaluations des facteurs relatifs à la vie privée : Archivé – Filtrage des personnes à surveiller à l'aide de caméras multiples », 22 juillet 2016. Consultation le 22 juillet 2021. <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/fotm-fra.html>.

⁵⁵ Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014... », p. 21 [OSSNR_202002_072, p. 21].

⁵⁶ Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014... », p. 21 [OSSNR_202002_072, p. 21].

⁵⁷ Le CPVP définit les fichiers de renseignements personnels comme « des descriptions de renseignements personnels relevant d'une institution fédérale qui sont organisés et qui peuvent être récupérés par le nom d'une personne ou par un numéro, un symbole ou d'autres éléments qui identifient cette personne. Les renseignements personnels décrits dans un FRP ont été utilisés, sont utilisés ou sont disponibles à des fins administratives. Le FRP décrit la manière dont les renseignements personnels sont recueillis, utilisés, divulgués, conservés ou éliminés dans le cadre de l'administration d'un programme ou d'une activité d'une institution fédérale. » Commissariat à la protection de la vie privée, « Sources de renseignements du gouvernement fédéral et sur les fonctionnaires fédéraux du Commissariat », 24 octobre 2019. Consultation le 20 août 2021. <https://www.priv.gc.ca/fr/a-propos-du-commissariat/acces-a-l-information-et-protection-des-renseignements-personnels-au-commissariat/infosource/>.

⁵⁸ ASFC, « Renseignements sur les programmes et les fonds de renseignements », 2 octobre 2019. Consultation le 28 septembre 2021. <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/infosource-fra.html>.

43. En fait, l’affichage et les avis publics au sujet des caméras ont été limités pendant la période de démonstration. La signalisation à l’aérogare 3 de l’aéroport international Pearson à Toronto indiquait que l’aire était sous vidéosurveillance, mais sans faire mention de la reconnaissance faciale⁵⁹. De même, la version du 19 novembre 2012 de l’énoncé de confidentialité de l’ASFC sur la surveillance et l’enregistrement visuels, mentionné dans l’EFVP du FOTM précise que les [traduction] « caméras peuvent [...] surveiller le mouvement des voyageurs et des marchandises d’un point d’opération de l’ASFC à un autre, par exemple d’un point primaire à un point secondaire⁶⁰ », mais sans faire mention d’une capacité de reconnaissance faciale⁶¹. Ces lacunes des dispositions relatives à l’énoncé de confidentialité semblent avoir été reconnues dans le rapport final sur le FOTM, où il est indiqué que la composante d’apprentissage automatique [traduction] « pourrait nécessiter une extension des protocoles actuels [de protection de la vie privée et de la sécurité]⁶² ».
44. À ce jour, le projet FOTM ou un type semblable de reconnaissance faciale n’a pas été adopté à titre permanent. D’autres priorités opérationnelles, dont la mise en place de bornes d’inspection primaire (BIP) dans certains aéroports⁶³, l’ont emporté à l’époque où le projet était en cours et l’ASFC n’a pas indiqué avoir des plans pour relancer le FOTM⁶⁴. La technologie en question a été retirée de l’aéroport à la fin du projet pilote⁶⁵.
45. L’ASFC s’est appuyé sur les pouvoirs de contrôle conférés par les articles 15 à 18 de la LIPR pour autoriser le projet FOTM en expliquant que [traduction] « ces articles exigent de quiconque entre au Canada qu’il subisse un examen de sa personne et de ses documents » et [traduction] « qu’ils permettent la présentation d’une preuve photographique de l’identité du demandeur »⁶⁶. En fait, le paragraphe 15 (3) de la LIPR dit « L’agent peut fouiller tout moyen de transport amenant des

⁵⁹ Le texte intégral de l’avis était : [traduction] « Cette aire fait l’objet de vidéosurveillance. Les enregistrements peuvent être utilisés et partagés conformément aux lois fédérales applicables. Pour en savoir plus sur l’utilisation que fait l’ASFC de ces enregistrements, veuillez demander à parler à un superviseur ou consulter le site www.cbsa-asfc.gc.ca. » ASFC, « Sommaires des évaluations des facteurs relatifs à la vie privée : Archivé – Filtrage des personnes à surveiller à l’aide de caméras multiples », 14 janvier 2016. Consultation le 15 septembre 2021. <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiipr/FOTM-fra.html>, p. 23.

⁶⁰ Face4 Systems Inc., « Faces on the Move: Multi-Camera Screening », p. 7.

⁶¹ ASFC, « Sommaires des évaluations des facteurs relatifs à la vie privée : Archivé – Filtrage des personnes à surveiller à l’aide de caméras multiples ».

⁶² Dans le rapport final sur le FOTM, on observe ce qui suit : [traduction] « Les protocoles de confidentialité et de sécurité applicables aux caméras de surveillance sont bien établis en ce qui concerne la notification, la visualisation, l’utilisation, le stockage et l’élimination. L’avènement de l’identification assistée par machine peut nécessiter une modification des protocoles actuels. » (Nous soulignons.) [OSSNR_202002_072, p. 2]

⁶³ Les bornes d’inspection primaire comportent aussi un recours à la biométrie; il en sera question aux paragraphes 125 à 137 du présent rapport

⁶⁴ Réponse écrite de l’ASFC à l’OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

⁶⁵ Réponse écrite de l’ASFC à l’OSSNR, 1^{er} octobre 2021.

⁶⁶ Réponse écrite de l’ASFC à l’OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

personnes au Canada [...] inspecter les documents et pièces relatifs à celles-ci⁶⁷ ». L'article 16 ajoute : « L'auteur d'une demande au titre de la présente loi doit répondre véridiquement aux questions qui lui sont posées lors du contrôle, donner les renseignements et tous éléments de preuve pertinents et présenter les visas et documents requis⁶⁸. » Dans le cas d'un étranger, la preuve à produire comprend « les éléments de preuve pertinents [qui] visent notamment la photographie et la dactyloscopie⁶⁹ ». L'ASFC n'a pas sollicité d'évaluation juridique du ministère de la Justice (MJ) quant à l'application de ces pouvoirs au programme pilote FOTM⁷⁰.

46. L'OSSNR se préoccupe du fait que l'ASFC se fie à ces pouvoirs généraux de contrôle pour soumettre à la reconnaissance faciale les voyageurs circulant vers le point de traitement. Les pouvoirs législatifs sur lesquels s'appuie l'ASFC supposent une interaction manifeste entre le voyageur et les agents de l'ASFC, et la présentation consciente par les voyageurs de leurs documents individuels, empreintes digitales et photos pendant leur contrôle. L'OSSNR n'est pas convaincu que les articles 15 à 18 de la LIPR autorisent clairement la collecte des données biométriques faciales des voyageurs, surtout avant et après le point de contrôle officiel. Il est d'avis qu'on se doit d'obtenir d'autres avis juridiques pour garantir que le recours à la reconnaissance faciale dans les aéroports canadiens (ou ailleurs à la frontière) sera bien fondé sur les pouvoirs conférés par la loi à l'ASFC.
47. L'ASFC a expliqué, en ce qui a trait à la conformité du projet pilote avec l'article 8 de la *Charte*, qu'un avis juridique n'était pas nécessaire de la part du ministère de la Justice parce que [traduction] « aucun renseignement n'était recueilli qui ne relevait pas de la technologie des caméras en circuit fermé qu'emploie actuellement l'Agence⁷¹ ». Le projet pilote faisait appel à [traduction] « l'infrastructure de surveillance existante » et [traduction] « n'introduisait rien de plus (en audio ou en vidéo) aux points d'entrée »⁷². Ainsi, l'ASFC jugeait que le FOTM ne remettait pas en question la protection des renseignements personnels ni ne soulevait d'autres questions nécessitant une consultation juridique⁷³.
48. Comme nous l'avons décrit au paragraphe 39, les documents de ce projet indiquent cependant que de nouvelles caméras *avaient été* installées en prévision de la période de démonstration. Il faut aussi dire que de tels arguments sous-estiment les effets de la technologie de la reconnaissance faciale sur la vie privée. Le fait important n'est pas l'installation ou l'absence de nouvelles caméras, mais plutôt leur capacité même de reconnaissance faciale. Ce nouvel aspect de ce qui est recueilli comme données change, peut-on penser, l'objet de la recherche. Comme le CPVP l'a recommandé, les EFVP (et, aux yeux de l'OSSNR, les évaluations des pouvoirs conférés par la loi) devraient être reprises en cas d'utilisation de nouvelles technologies, de sorte qu'on

⁶⁷ LIPR, article 15(3); se reporter aussi à l'obligation légale de se soumettre à un contrôle en vertu du paragraphe 18(1).

⁶⁸ LIPR, paragraphe 16(1).

⁶⁹ LIPR, alinéa 16(2)b).

⁷⁰ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

⁷¹ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

⁷² Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

⁷³ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 6 – Innovation Projects & VRP », p. 3.

soit sûr de bien comprendre l'objet de la recherche – et ses conséquences sur la vie privée⁷⁴. On devrait renouveler les avis au public pour être sûr que le recours à la reconnaissance faciale est nettement connu de la population, sauf là où les nécessités du service justifient un moindre degré de transparence.

49. Nous nous devons d'étudier avec soin la mise en place d'une telle technologie à court ou à long terme et veiller à ce que ce déploiement repose pleinement sur des pouvoirs conférés par la loi et une solide politique-cadre. Le FOTM a démontré les avantages réels qu'il présente pour l'exécution des fonctions de l'ASFC à la frontière, plus particulièrement l'identification des gens qui posent un problème. Il est connu que des gens déjà expulsés pour des raisons d'interdiction de territoire peuvent tenter d'entrer à nouveau au Canada sous une identité usurpée ou fausse. C'est ce dont témoignent les 47 « correspondances » établies pendant les six mois de la période de démonstration du projet FOTM. Ainsi qu'il a été noté dans d'autres contextes, il est sûr que la sécurité nationale n'est qu'un des nombreux intérêts visés par une meilleure gestion de l'identité. Ajoutons que les décisions d'interdiction de territoire pour cause de sécurité (selon l'article 34 de la LIPR) constituent une fraction relativement modeste de toutes les décisions en matière d'interdiction de territoire⁷⁵. Il ne faut pas oublier pour autant que même les faits rares peuvent avoir des conséquences extrêmes. Les cas d'atteintes à la sécurité nationale sont, de nature, peu fréquents, mais sérieux.

Projet FASTER-PrivBio (2015-2017)

50. FASTER-PrivBio est un projet de « validation de principe » dans le cadre duquel un prototype d'application mobile devant faciliter la demande et l'octroi d'autorisations de voyage électroniques (AVE)⁷⁶ a été créé. Il a été mené par IRCC avec l'ASFC et d'autres partenaires (dont l'Université d'Ottawa et l'Université Ryerson). Cette application permettait de prendre une photo numérique (en autoportrait), d'extraire la photo numérique du passeport à puce, de comparer les deux clichés par reconnaissance faciale (vérification individuelle) et de confirmer l'authenticité

⁷⁴Voir les paragraphes 36 à 38 de Commissariat à la protection de la vie privée, « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée », 10 juin 2021. Consultation le 13 septembre 2021. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/.

⁷⁵ Ainsi, les allégations en vertu de l'article 34 ont figuré pour 2,74 % (11 sur 402) des enquêtes sur l'interdiction de territoire de la Commission de l'immigration et du statut de réfugié (CISR) de janvier à mars 2021. En 2020, le pourcentage s'est établi à 4,26 % (44 sur 1 034). Voir Commission de l'immigration et du statut de réfugié du Canada, « Enquêtes réglées selon le type d'allégations », 30 août 2021. Consultation le 15 septembre 2021. <https://irb.gc.ca/fr/statistiques/enquetes/Pages/AdmHalle.aspx>.

⁷⁶ L'AVE est une exigence à l'entrée pour les ressortissants étrangers dispensés de l'obligation de visa qui se rendent au Canada par avion. Les visiteurs font une demande en ligne avant leur arrivée au pays en fournissant certains renseignements biographiques et en répondant à plusieurs questions de contrôle. Une fois accordée, l'AVE est jointe au passeport du voyageur.

du document de voyage. Une fois l'inscription réussie, l'application créait un « jeton d'accès » destiné à faciliter les mouvements dans le continuum frontalier pour les voyageurs à faible risque⁷⁷. Le projet comportait un cadre de « protection de la vie privée dès la conception » en mettant l'accent sur la prise en charge des problèmes de confidentialité que pose le recours à la biométrie⁷⁸.

51. Deux atouts de base étaient envisagés en matière de sécurité. La facilitation des mouvements des voyageurs à faible risque permettrait de concentrer les ressources et l'attention ailleurs, notamment en direction des voyageurs à plus grand risque dans le cadre du traitement manuel. Second avantage, l'application contrôlerait automatiquement les voyageurs inscrits au moyen des listes biographiques de surveillance applicables (de l'ASFC, d'IRCC et d'autres organismes comme l'Organisation internationale de police criminelle [INTERPOL]), permettant ainsi l'identification des personnes préoccupantes⁷⁹. Cette dernière fonction ferait cependant double emploi dans une large mesure avec le contrôle existant dans le processus AVE.
52. Le projet a pris fin en 2017 après avoir su démontrer l'obtention des avantages attendus⁸⁰. Parmi les principaux points à en retenir, mentionnons la viabilité (sur téléphone intelligent) des justificatifs d'identité biométriques mobiles avec des protections suffisantes de sécurité des données selon les participants au projet, la compatibilité avec les passeports électroniques et les systèmes et l'infrastructure connexes d'IRCC, et les solides vérifications d'identité rendues possibles par un tel système⁸¹. L'étape qui a suivi dans ce projet était de travailler à une mise en

⁷⁷ Alex Stoianov, « Technical Report 4: FasterPriv Bio : The Policy Analysis », Université Ryerson, février 2017, p. 26 [OSSNR_202002_082, p. 26]. Le rapport de clôture du projet indiquait que [traduction] « l'application mobile devrait apporter plus de commodité aux [...] voyageurs » en leur permettant de [traduction] « passer à la frontière plus rapidement, plus efficacement et plus facilement ». Recherche et développement pour la défense Canada (RDDC), « FASTER-PrivBio Project Summary Report », octobre 2018. Consultation le 20 août 2021. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc331/p808727_A1b.pdf, p. 9.

⁷⁸ « Technical Report 3: FasterPriv Bio : The Privacy Analysis: A Case Study in Privacy by Design », Université Ryerson, mars 2017 [OSSNR_202002_080]. La grande caractéristique relativement à la vie privée était la « décentralisation » du stockage des données biométriques. Plutôt que de recueillir et de verser une image faciale dans une base d'information centralisée, cette image était conservée par l'utilisateur et vérifiée au besoin à l'aide d'un modèle anonymisé. Un stockage décentralisé des données biométriques est généralement jugé préférable du point de vue de la protection de la vie privée, parce qu'il diminue le risque d'atteintes aux données.

⁷⁹ Programme canadien pour la sûreté et la sécurité, « CSSP-2015-CP-2114 : FasterPriv Bio », sans date, p. 1 [OSSNR_202002_085, p. 1]. Ce projet de validation de principe a démontré la capacité de l'application mobile à reproduire le contrôle exercé dans le processus type de l'AVE; la recherche dans de nouvelles bases de données consacrées à la biométrie n'était pas incluse ni envisagée dans le projet. Voir « Technical Report 3: FasterPriv Bio : The Privacy Analysis » [OSSNR_202002_080].

⁸⁰ RDDC, « FASTER-PrivBio Project Summary Report », p. 9.

⁸¹ RDDC, « FASTER-PrivBio Project Summary Report », p. 9.

service dans le cadre de l'initiative « Chaîne de confiance » (CdC). Cette initiative en cours est décrite à la section **Error! Reference source not found.**, paragraphes 151-155 plus loin.

Projet d'expansion de la biométrie (2015-2020)

53. Lancé en 2015, le Projet d'expansion de la biométrie (PEB) a constitué, comme son nom l'indique, un autre grand pas en avant dans la collecte de données biométriques aux fins de l'immigration. S'inspirant du PBRT, le PEB a étendu la collecte de données biométriques à l'ensemble des personnes (sauf dispense) qui présentent une demande ou une requête en vertu de la LIPR⁸². Il a intégré l'initiative ERI et étendu l'échange automatisé de renseignements sur l'immigration, notamment par l'interrogation de données biométriques, aux partenaires étrangers du groupe des 5 pour les migrations (M5) avec les organismes s'occupant d'immigration aux États-Unis, en Australie, en Nouvelle-Zélande et au Royaume-Uni⁸³. Il a également élargi la capacité de vérification des empreintes digitales aux points d'entrée canadiens (PDE) en instaurant un mode automatisé VSED (vérification systématique des empreintes digitales) dans huit aéroports internationaux (voir le paragraphe 73) et en ajoutant une vérification

⁸² Pour la liste complète des pays à dispense d'obligation de visa, voir l'annexe 1.1 du RIPR à <https://laws-lois.justice.gc.ca/PDF/DORS-2002-227.pdf>. Consultation le 17 août 2021. Voir aussi gouvernement du Canada, « Exigences d'admission selon le pays ou territoire », 29 novembre 2019. Consultation le 17 août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/services/visiter-canada/exigences-admission-selon-pays.html>.

⁸³ Le Groupe des 5 pour les migrations (M5), auparavant un forum consultatif, est devenu un organisme axé sur l'action et la collaboration avec des initiatives communes et des échanges d'information visant à améliorer la sécurité, le service et les économies. Le M5 est soutenu par un secrétariat permanent hébergé en Nouvelle-Zélande et doté de toutes les ressources nécessaires par ce pays. Le Canada est représenté au M5 aussi bien par IRCC que par l'ASFC.

discrétionnaire à l'inspection secondaire dans 11 autres aéroports et 40 points d'entrée terrestres⁸⁵.

54. Le PEB a pris fin en 2020 et les activités biométriques qu'il a instaurées sont devenues des opérations établies. Les activités en question sont décrites à la section **Error! Reference source not found.**, paragraphes 63 à 94 plus loin.

Évaluation du *passé de la biométrie*

55. Dans cette section, nous avons examiné l'évolution des dernières décennies des activités biométriques dans le continuum frontalier en mettant en lumière les grands moments, programmes et projets pilotes dont cette évolution a été jalonnée. Considérées collectivement, ces activités dégagent un certain nombre de thèmes.
56. Premièrement, la collecte et l'utilisation de données biométriques n'ont cessé d'évoluer au gouvernement du Canada. Dans le contexte de l'immigration par exemple, elles ne concernaient d'abord que les personnes expulsées et les demandeurs d'asile en 1993, pour éventuellement, en 2018 viser l'ensemble des auteurs (sauf dispense⁸⁶) de demandes ou de requêtes en vertu de la LIPR.
57. Deuxièmement, les engagements et les priorités arrêtés à la suite des attentats du 11 septembre ont stimulé l'adoption de la biométrie au début du millénaire, jetant les bases de ce qui est aujourd'hui l'architecture fondamentale des activités biométriques dans le continuum frontalier. Dans ce contexte, la raison d'être de l'adoption de la biométrie était la sécurité nationale. Identifier les gens signifiait identifier les terroristes potentiels.
58. Troisièmement, l'identification des gens est aussi (et de plus en plus) une question de gestion plus générale de l'identité. Pour l'ASFC et IRCC, la biométrie contribue à la réalisation des objectifs généraux de l'organisme, et non des seuls objectifs en matière de sécurité nationale. À mesure que les événements du 11 septembre sont devenus choses du passé, cette gestion plus générale de l'identité a tenu relativement plus de place dans la justification de la collecte et de l'utilisation de données biométriques. Ce changement s'est traduit par une logique plus équilibrée de cette adoption où on s'attachait à l'utilité globale plutôt qu'à l'aspect moindre – quoique important – de la sécurité nationale.
59. Quatrièmement, à mesure que les activités biométriques prenaient de l'ampleur, le chevauchement et/ou le partage de la responsabilité de leur conception et de leur application gagnaient en importance, qu'il s'agisse des rapports entre ministères et organismes publics (IRCC et ASFC, par exemple), entre pays (Canada et États-Unis ou autres partenaires internationaux) ou entre secteurs public et privé (mobilisation des partenaires de l'industrie par le gouvernement du Canada). Ce resserrement de la collaboration pourrait avoir des conséquences sur les droits individuels à la vie privée et les futurs usages possibles de la biométrie; il fait aussi ressortir l'importance d'une bonne sécurité des données parmi les diverses institutions.

⁸⁵ IRCC, « Biometrics Expansion Project: Project Close Out Report », 16 juillet 2020, p. 1 [OSSNR_202002_027, p. 1].

⁸⁶ Pour une liste des dispenses, voir la note 91.

60. Cinquièmement, la facilitation des mouvements est devenue un autre facteur d'adoption de la biométrie, le but étant d'accroître l'efficacité à la frontière et de tenir compte de l'évolution des normes de la société en matière d'utilisation de la technologie. Comme le suggère le projet FASTER-PrivBIO, on tient pour acquis que les voyageurs connaissent bien les appareils numériques au moment de mettre en place de nouvelles activités biométriques. Il faut aussi dire que les gens adopteront plus volontiers des technologies relativement intrusives si l'adhésion est volontaire et consensuelle⁸⁷. La tension observée – entre les attentes respectives de commodité et de confidentialité – façonnera sans doute à l'avenir le débat public sur la biométrie.
61. Sixièmement et relativement à ce qui précède, l'expansion de la biométrie a coïncidé avec une insistance grandissante sur la vie privée et ses protections. Nombre de projets et d'initiatives pilotes que nous avons décrits dans cette section répondent expressément à ces préoccupations, notamment en adoptant ce qu'on appelle les principes de « protection de la vie privée dès la conception », lesquels visent à protéger proactivement les renseignements personnels⁸⁸. Cette dynamique reflète l'évolution dans le temps d'une compréhension plus large (de la part du gouvernement, de l'industrie, du milieu juridique ou du milieu universitaire) des risques particuliers qui sont liés à la collecte et à l'utilisation des données biométriques. Certaines applications de l'analyse biométrique – par exemple, la reconnaissance faciale dans le projet FOTM – présentent plus de risques que les autres et doivent être examinées en conséquence..

5. BIOMÉTRIE ACTUELLE

62. Cette section traitera des activités biométriques établies du gouvernement du Canada dans le continuum frontalier. Il sera aussi question du rôle de la biométrie dans le Programme d'immigration et le Programme de passeport respectivement. Dans chaque cas, nous examinerons comment la biométrie contribue à l'atteinte des objectifs de ces programmes (en évoquant, s'il y a lieu, la collecte, l'utilisation, la conservation et la communication de données biométriques) et considérerons les critères énoncés à la section 3. À la fin de cette section, nous examinerons le processus de l'« arrivée au Canada » avec l'analyse des données biométriques

⁸⁷ Ainsi, un sondage réalisé par l'Association du transport aérien international (IATA) en 2019 a révélé que 70 % des voyageurs étaient prêts à partager des renseignements personnels supplémentaires, y compris leurs identificateurs biométriques, afin d'accélérer les processus à l'aéroport. IATA, « Global Passenger Survey (2019) », Consultation le 3 octobre 2021. <https://www.iata.org/en/pressroom/pr/2019-10-16-01/>.

⁸⁸ Voir, par exemple, les principes énoncés dans Ann Cavoukian, « Privacy by Design : The 7 Foundational Principles », janvier 2011. Consultation le 20 août 2021. <https://www.iapp.org/lang/fr>.

des voyageurs et des participants à NEXUS aux bornes automatisées des aéroports canadiens. Tout au long, nous exposerons enfin les considérations utiles en matière de sécurité nationale.

Programme d'immigration

63. IRCC est chargé du contrôle de l'admissibilité des candidats à la résidence permanente ou temporaire qui arrivent au Canada⁸⁹. Dans ce processus (que nous appellerons le « Programme d'immigration »), IRCC recourt à la biométrie avec la collaboration de l'ASFC et de la GRC. Comme IRCC a indiqué à l'OSSNR, [traduction] « IRCC recueille, la GRC stocke et l'ASFC vérifie⁹⁰ ».
64. IRCC recueille les empreintes des (dix) doigts et prend une photo numérique aux fins des demandes de statut ou de visa de résident temporaire et de permis de travail, d'études ou de résidence temporaire, des demandes de résidence permanente et des demandes d'asile et de réinstallation de réfugiés⁹¹. Les données biométriques recueillies sont versées dans deux bases de données : les photos vont dans le Système mondial de gestion des cas (SMGC) d'IRCC et les empreintes digitales, dans le Système automatisé d'identification dactyloscopique (SAID)⁹². La photo numérique, bien que conforme aux règles de l'OACI, ne sert pas à la reconnaissance faciale et pourrait ne pas être d'une qualité suffisante pour ce genre d'analyse. Nous nous

⁸⁹ Gouvernement du Canada, « Mandat et rôle [IRCC] », 10 mars 2020. Consultation le 17 août 2021.

<https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/publications-guides/plan-ministeriel-2020-2021/mandat-role.html>.

⁹⁰ Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 5.

⁹¹ Il existe un certain nombre de dispenses à l'obligation de fournir des données biométriques. Sont visées les demandes de citoyens canadiens, de membres des Premières Nations inscrits et de gens déjà admis à la résidence permanente au Canada, de visiteurs dispensés de l'obligation de visa qui sollicitent une autorisation de voyage électronique (AVE), d'étrangers de moins de 14 ans ou de plus de 79 ans (il n'existe aucune limite supérieure d'âge pour les demandeurs d'asile au Canada même), de ressortissants américains sollicitant un permis de travail, d'études ou de résidence temporaire, de Sa Majesté la Reine et tout membre de la famille royale sollicitant un permis de travail, d'études ou de résidence temporaire, de ressortissants d'autres pays qui sont titulaires d'un visa en règle d'entrée aux États-Unis et qui transitent par le Canada pour moins de 48 heures à destination ou en provenance des États-Unis directement, de ministres et de représentants et diplomates accrédités d'autres pays (et des membres de leur famille) venant au Canada dans l'exercice de leurs fonctions et de chefs d'État ou de gouvernement en séjour temporaire à des fins officielles ou non. Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 2. La pandémie de COVID-19 a nui à la collecte de données biométriques; notamment l'obligation de fournir des données biométriques dans certains contextes a été suspendue, bien que tous les changements en ce sens doivent être de nature temporaire. Ainsi, les demandeurs de résidence temporaire se trouvant au Canada au moment de leur demande sont provisoirement dispensés de la même obligation et, pour les demandes de résidence permanente, il est possible d'utiliser des données biométriques déjà recueillies (si elles ont été prises au cours des 10 dernières années). Voir gouvernement du Canada, *Maladie à coronavirus (COVID-19) : Biométrie*, 1^{er} juin 2021. Consultation le 28 juillet 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/services/coronavirus-covid19/biometrie.html>.

⁹² Le SAID est un sous-système du Système d'identification en temps réel (SITR) de la GRC, qui facilite le stockage et le traitement électronique des empreintes digitales des criminels, des réfugiés, des candidats à l'immigration, des membres du personnel et des civils. Réponse écrite de la GRC à l'OSSNR, 31 mai 2021, p. 11.

intéresserons donc surtout aux empreintes digitales dans notre description et notre analyse des activités.

65. Les données biométriques sont recueillies et inscrites en divers points de service au Canada comme à l'étranger, le plus souvent (90 % des fois environ) dans les centres de réception des demandes de visa (CRDV). Les CRDV relèvent de fournisseurs de services commerciaux. Ils sont gérés par des entreprises privées et leurs services sont retenus à forfait par IRCC pour l'inscription biométrique à l'étranger.
66. Le stade de la collecte est une étape délicate compte tenu du caractère personnel des données biométriques. Les grandes préoccupations ont à voir avec la confidentialité et la sécurité des données biométriques. Les médias ont fait état de préoccupations au sujet des CRDV en mettant en doute la possibilité d'assurer une protection suffisante des données personnelles en raison du rôle central joué par des entrepreneurs privés établis à l'extérieur du Canada⁹³. Il y a aussi eu examen des liens possibles entre le sous-traitant administrant le CRDV du Canada à Beijing et les forces de sécurité chinoises⁹⁴. Les gouvernements étrangers ont intérêt à savoir qui demande à venir au Canada – information qui peut servir à surveiller, à réprimer, à harceler, à contraindre, à menacer ou à léser les intéressés. Le risque d'interception ou de vol de données biométriques est particulièrement préoccupant du fait de leur usage possible à des fins d'observation, de surveillance et d'identification.
67. IRCC a pris des mesures pour exercer un contrôle sur la circulation des renseignements biométriques (ce qui comprend la collecte et la communication de ces données) dans les CRDV. Les contrats passés avec les fournisseurs des CRDV énoncent l'obligation pour eux de respecter les lois canadiennes sur la protection des renseignements personnels⁹⁵. IRCC mentionne également que ces fournisseurs font l'objet d'une surveillance de représentants canadiens par voie d'audit et d'examen sur place des CRDV⁹⁶. Il signale que toutes les données biométriques recueillies hors du Canada seraient chiffrées avant d'être transmises aux serveurs du Ministère en sol canadien (photos dans le SMGC), ainsi qu'à la GRC (empreintes digitales dans le SAID). IRCC ajoute que, une fois bien transmis, les renseignements sont supprimés au point de collecte⁹⁷.
68. Vu la nature des activités menées dans certains pays étrangers, il demeure difficile de préserver les renseignements que fournissent les demandeurs dans les CRDV. Certains centres se trouvent dans des pays aux intérêts nationaux incompatibles avec ceux du Canada. Les conséquences sur la sécurité nationale des atteintes à la sécurité dans ces CRDV peuvent donc être

⁹³ Voir Andrew Russell et Max Hartshorn, « Canada paid nearly \$200M to visa company previously based in a tax haven and linked to China », *Global News*, 3 février 2021. Consultation le 14 août 2021. <https://globalnews.ca/news/7563381/canada-visa-application-firm-tax-haven-ties-china/>

⁹⁴ Voir Nathan Vanderklippe et Steven Chase, « Canada's visa application centre in Beijing run by Chinese police », *Globe and Mail*, 8 février 2021. Consultation le 13 août 2021. <https://www.theglobeandmail.com/world/article-canadas-visa-application-centre-in-beijing-run-by-chinese-police/>

⁹⁵ Travaux publics et Services gouvernementaux Canada, demande de propositions pour le renouvellement du contrat relatif au réseau mondial de CRDV pour la biométrie du Programme d'immigration, p. 23 [IRCC DR n° 2 Documents].

⁹⁶ Réponse écrite d'IRCC à l'OSSNR, 1^{er} octobre 2021.

⁹⁷ Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 8.

particulièrement graves. Bien que la portée de la présente étude n'ait pas permis d'examiner en profondeur les mesures de sécurité dans les CRDV, l'OSSNR pourrait vouloir revenir sur la question plus tard.

69. Dans le continuum frontalier, le Canada tire parti (ou fait usage) des données biométriques recueillies de trois manières : contrôle à l'inscription (avec tout renseignement renvoyé permettant d'éclairer la décision sur une demande), vérification à l'arrivée à un point d'entrée au Canada et évaluation continue de l'admissibilité (ou du statut d'immigration) postérieurement à l'arrivée.
70. Le contrôle des empreintes digitales à l'inscription est automatique et fait appel à des bases de données tant du Canada que de l'étranger. À l'inscription, IRCC ou l'ASFC⁹⁸ soumet les empreintes digitales prises à la GRC. Les empreintes et les données biographiques sont alors comparées avec les données des répertoires dactyloscopiques de la criminalité et de l'immigration à la GRC (cela comprend dans ce dernier cas les empreintes digitales prises dans le cadre de demandes antérieures). La recherche se fait en outre dans les bases de données d'immigration des pays du M5 partenaires du Canada⁹⁹.
71. Les renseignements obtenus lors du contrôle dans les bases de données au pays et à l'étranger éclairent les décisions d'admissibilité et permettent de déceler les cas possibles d'interdiction de territoire pour raisons de sécurité en vertu de l'article 34 de la LIPR¹⁰⁰. Le partage des renseignements biométriques sur l'immigration avec les pays partenaires du M5 comprend l'échange de codes d'avertissement liés à des renseignements préjudiciables. Les renseignements sur un problème possible de sécurité nationale peuvent être transmis à une organisation du portefeuille de la Sécurité publique (notamment le SCRS et l'ASFC) pour un contrôle de sécurité supplémentaire. Le contrôle à l'étranger se fait aussi à l'aide de renseignements biographiques¹⁰¹, mais les données biométriques offrent comme autre avantage de dégager les correspondances dans le cas des demandes antérieures sous des noms différents et/ou en cas de renseignements biographiques divergents.

⁹⁸ Les voyageurs dispensés de l'obligation de visa peuvent demander un permis d'études ou de travail à leur arrivée au point d'entrée, auquel cas l'ASFC est chargé de la collecte et de l'inscription des données biométriques.

⁹⁹ IRCC, « PIA - Migration Five Information Sharing Regulations », sans date [IRCC DR n° 2 Documents].

¹⁰⁰ L'article 34 dit : « Emportent interdiction de territoire pour raison de sécurité les faits suivants : a) être l'auteur de tout acte d'espionnage dirigé contre le Canada ou contraire aux intérêts du Canada; b) être l'instigateur ou l'auteur d'actes visant au renversement d'un gouvernement par la force; b.1) se livrer à la subversion contre toute institution démocratique, au sens où cette expression s'entend au Canada; c) se livrer au terrorisme; d) constituer un danger pour la sécurité du Canada; e) être l'auteur de tout acte de violence susceptible de mettre en danger la vie ou la sécurité d'autrui au Canada; f) être membre d'une organisation dont il y a des motifs raisonnables de croire qu'elle est, a été ou sera l'auteur d'un acte visé aux alinéas a), b), b.1) ou c) ». Disponible à : <https://laws-lois.justice.gc.ca/fra/lois/i-2.5/page-5.html>. Consultation le 17 août 2021.

¹⁰¹ Le contrôle biographique dans les bases de données étrangères se fait en-dehors et en sus du processus de contrôle dactyloscopique. Le rôle de la GRC dans ce contexte se limite à une vérification anonyme des empreintes digitales auprès des partenaires du M5.

72. À la suite du processus de contrôle, l'ASFC se reporte aux données biométriques pour vérifier l'identité des ressortissants inscrits qui arrivent à un point d'entrée au Canada. On s'assure ainsi – avec un degré d'assurance généralement impossible sans un recours aux données biométriques – que la personne qui se voit accorder un visa ou un permis est réellement celle qui entre au Canada.
73. Le mode de vérification varie selon les points d'entrée. Dans huit aéroports internationaux, il y a vérification systématique des empreintes digitales (VSED) aux bornes d'inspection primaire (BIP). Ce sont des bornes automatisées de traitement des voyageurs qui passent par la douane et l'immigration dans les grands aéroports canadiens (pour plus de détails sur les BIP, voir les paragraphes 125 à 137 plus loin). La borne d'inspection primaire capte les empreintes digitales et transmet les données biométriques à la GRC en vue d'une vérification individuelle avec la référence dactyloscopique du voyageur dans la base de données de la Gendarmerie royale du Canada¹⁰³. Si le service VSED n'est pas disponible, les agents des services frontaliers (ASF) vérifient l'identité en comparant la photo inscrite du voyageur à la personne qui se présente devant eux, tandis que la vérification des empreintes digitales se fait à titre discrétionnaire à l'inspection secondaire au moyen des appareils LiveScan de l'ASFC¹⁰⁴.
74. La biométrie sert également à évaluer le maintien de l'admissibilité. En d'autres termes, elle constitue un moyen de faire le lien entre les gens et les renseignements susceptibles d'influer sur leur statut d'immigration et/ou de futures demandes d'immigration (démêlés avec les forces de l'ordre, par exemple, qui pourraient indiquer une interdiction de territoire).
75. La période de conservation des données biométriques recueillies dépend en partie du résultat de la demande. Dans le cas des demandes de résidence tant temporaire¹⁰⁵ que permanente refusées pour des raisons d'« interdiction de territoire » qu'IRCC juge graves (articles 34 à 37 de la LIPR), les données biométriques sont conservées jusqu'au 100^e anniversaire de l'intéressé.
76. Cette longue période de conservation offre des avantages en matière de sécurité, car les données biométriques peuvent permettre de déceler toute demande ultérieure présentée par l'intéressé à un certain moment (réaliste) dans l'avenir, même sous un nom différent. Elle rend aussi

¹⁰³ En plus des empreintes digitales saisies, la BIP envoie un numéro de référence unique créé à l'inscription, de sorte que la bonne fiche dactyloscopique puisse être extraite à des fins de comparaison. Les résultats de la comparaison individuelle sont normalement renvoyés dans les cinq secondes.

¹⁰⁴ LiveScan est un appareil de lecture et de communication électroniques des empreintes digitales. Ce système comprend une double interface matérielle et logicielle de transmission de l'information.

¹⁰⁵ Cela comprend les visas de résident temporaire et les permis d'études, de travail et de résidence temporaire.

l'identification possible pour les partenaires au pays ou à l'étranger qui sont autorisés à interroger la base de données sur l'immigration. Si quelqu'un fait l'objet d'une suspension de casier judiciaire, d'une réhabilitation pénale ou d'une dispense ministérielle, la période de conservation est normalement ramenée à 15 ans (période standard) à compter de la date d'inscription des données biométriques. C'est là un élément important, car il ramène la période de conservation à la période standard une fois les circonstances ayant justifié une conservation prolongée éliminées.

77. À la fin de la période de conservation, l'information biométrique est éliminée par IRCC conformément aux autorisations applicables émanant de Bibliothèque et Archives Canada. Pour ce qui est des empreintes digitales détenues par la GRC, une demande de purge électronique est transmise par IRCC et une confirmation de la suppression est renvoyée¹⁰⁶.
78. En 2021, IRCC a découvert une atteinte à la vie privée qui était liée à la conservation de données dactyloscopiques et de photos de l'immigration au-delà de la période de conservation prescrite. Les données appartenaient à des gens qui ont accédé à la citoyenneté canadienne, ce qui créait l'obligation, suivant la politique de conservation des données biométriques d'IRCC, de supprimer les empreintes digitales et les photos au dossier de l'immigration des intéressés. IRCC a informé le CPVP de la question en février 2021 et a avisé les clients touchés par courriel en mars de la même année¹⁰⁷. Un avis public a été diffusé sur le site Web d'IRCC¹⁰⁸.
79. La communication de renseignements biométriques soulève des préoccupations en matière de protection de la vie privée et exige un examen attentif de leur utilisation ultérieure. Comme les données biométriques sont des renseignements personnels, le cadre juridique en place exige que le gouvernement du Canada les emploie uniquement aux fins pour lesquelles elles ont été obtenues (à savoir la décision sur l'admissibilité à entrer ou à demeurer au Canada), à des fins compatibles ou à des fins autrement autorisées par la loi.
80. Les recherches automatisées entre le Canada et ses partenaires du M5 sont une recherche (dactyloscopique) biométrique anonyme sans transmission d'informations biographiques; en cas de correspondance, les renseignements utiles sur l'immigration sont transmis et, dans le cas contraire, le pays en question renvoie un résultat nul. Dans l'un et l'autre cas, le pays qui reçoit la demande de recherche est tenu de purger les données dactyloscopiques et donc de ne pas les conserver¹⁰⁹. Le système est conçu en définitive dans l'intention d'exclure les échanges de données biographiques et/ou de renseignements sur l'immigration sauf si les deux parties

¹⁰⁶ Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 10.

¹⁰⁷ Signalons que la conservation des renseignements de certains clients a donné lieu à la communication de cette information aux organismes d'application de la loi. « Bio Purge Privacy Breach information provided to CIMM June 2 2021 », p. 3 [IRCC DR n° 2 Documents].

¹⁰⁸ IRCC, « Bio Purge Privacy Breach information provided to CIMM June 2 2021 », [IRCC DR n° 2 Documents]. Pour l'avis public, voir Gouvernement du Canada, « Lettre ou courriel envoyé aux clients pour les informer de la consultation des données biométriques », 19 mars 2021. Consultation en ligne le 5 août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/nouvelles/avis/courriel-lettre-envoye-conservation-donnees-biometriques.html>.

¹⁰⁹ Chaque entente bilatérale précise qu'une conservation du genre ne convient pas et prévoit des mesures d'« assurance de la qualité » pour contrôler la situation et s'assurer que cette conservation n'a pas lieu. Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 3.

détiennent déjà des données biométriques connexes dans leurs bases de données, ce qui constitue une importante mesure de protection de la vie privée. De plus, les ententes de recherche automatisée précisent que tout renseignement échangé portera uniquement sur des tiers étrangers. En d'autres termes, le Canada n'enverra ni ne recevra de renseignements sur des citoyens canadiens ou sur des résidents permanents au pays sauf s'il s'agit de demandes d'asile.

81. Des échanges moins fréquents au cas par cas (ou *ponctuels*) peuvent consister en l'échange de renseignements biométriques de base (photos ou empreintes digitales) si la partie requérante juge l'information utile à l'application de ses lois sur l'immigration et la citoyenneté¹¹⁰. Ces échanges s'accompagnent de mises en garde concernant l'utilisation, l'acheminement et la conservation qui valent pour tout renseignement communiqué (et non pour les seules données biométriques), mais sans que ces mises en garde soient juridiquement contraignantes pour les participants¹¹¹. IRCC a en outre indiqué que des échanges ponctuels de renseignements biométriques étaient possibles avec des partenaires internationaux autres que les pays membres du M5, [traduction] « si la personne à qui se rapportent ces renseignements y consent ou si l'alinéa 8 (2) a) [sur les usages compatibles] de la *Loi sur la protection des renseignements personnels* l'autorise¹¹² ».
82. Les principales sources d'habilitation de la collecte, de l'utilisation et de la communication de données biométriques dans le Programme d'immigration sont la LIPR et le RIPR (*Règlement sur l'immigration et la protection des réfugiés*). Plus précisément, l'article 10.01 de la LIPR autorise la collecte de données biométriques pour inscription et vérification en réponse à une demande en vertu de la loi. Suivant l'article 10.02, le ministre peut prendre des règlements sur la mise en œuvre de ces processus dans le cadre du RIPR. Ce règlement précise à qui s'appliquent les exigences en matière de biométrie, la nature des données biométriques en question et la façon de procéder à la collecte, au traitement et à la vérification¹¹³. Le paragraphe 16 (1) de la LIPR exige que l'auteur d'une demande au titre de la présente loi réponde véridiquement aux questions qui lui sont posées lors du contrôle et donne « les renseignements et tous éléments de preuve pertinents ». Le paragraphe 16 (2), qui s'applique uniquement aux étrangers, indique que les éléments de preuve à produire visent notamment « la photographie et la dactyloscopie ». IRCC cite également l'article 4 de la *Loi sur la protection des renseignements personnels* qui autorise la collecte des seuls renseignements personnels « qui ont un lien direct avec ses [IRCC] programmes ou ses activités ». Enfin, il indique que, conformément à l'article 7 de cette même loi, les données biométriques [traduction] « serviront uniquement aux fins pour lesquelles elles sont recueillies ou pour des usages compatibles avec ces fins¹¹⁴ ».

¹¹⁰ On trouvera les ententes en question à gouvernement du Canada, « Ententes et accords avec d'autres ministères et gouvernements », 27 mars 2018. Consultation le 17 août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/mandat/politiques-directives-operationnelles-ententes-accords/ententes.html>.

¹¹¹ Dans ce contexte, les empreintes digitales et les photographies faciales sont alors regroupées avec d'autres renseignements personnels (nom, date de naissance, adresse, renseignements médicaux, antécédents de voyage, etc.) sans autre apport (par des comparaisons entre bases de données) à des fins d'identification comme pour les échanges automatisés.

¹¹² Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 13.

¹¹³ Voir en particulier la partie 2, section 2.1.

¹¹⁴ Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 12.

83. Pour ce qui est de la communication par IRCC de données biométriques à ses alliés internationaux, l'article 7 de la LIPR autorise le ministre, avec l'agrément du gouverneur en conseil, à conclure un accord avec le gouvernement d'un État étranger aux fins de cette même loi. De multiples accords semblables relèvent du RIPR qui traite des activités de partage d'information du Canada avec chaque partenaire du M5¹¹⁵ : Accord entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique concernant l'échange de renseignements sur les visas et l'immigration¹¹⁶; Annexe concernant l'échange d'information sur les demandes d'asile et du statut de réfugié à la Déclaration d'entente mutuelle sur l'échange d'information; accords bilatéraux d'échanges automatisés conclus avec les gouvernements de l'Australie, de la Nouvelle-Zélande et du Royaume-Uni¹¹⁷. Ces accords prévoient la communication de données biographiques et biométriques entre les parties s'il s'agit de « renseignements nécessaires, pertinents et proportionnels à l'atteinte des objectifs de la présente section [administration et contrôle d'application des lois respectives des parties en matière de citoyenneté et d'immigration]¹¹⁸ ». Les dispositions de chaque entente régissent également la destruction de l'information et la correction des renseignements déjà reçus et confèrent au ministre le pouvoir discrétionnaire de refuser de communiquer une information préjudiciable aux intérêts nationaux du Canada¹¹⁹.
84. De telles communications seraient aussi conformes à l'alinéa 8 (2)f) de la *Loi sur la protection des renseignements personnels* qui permet la communication aux termes d'accords ou d'ententes conclus par le gouvernement du Canada avec un État étranger à des fins d'administration ou de contrôle d'application de ses lois¹²⁰. Les échanges *ponctuels* avec les partenaires en dehors du M5 se font conformément aux dispositions de l'alinéa 8(2)a) de cette même loi.
85. De plus, les organismes canadiens d'application de la loi peuvent avoir accès aux données dactyloscopiques recueillies par IRCC dans le traitement des demandes d'immigration à des fins de contrôle d'application de la loi. L'article 13.11 du RIPR autorise la GRC à utiliser – ou à communiquer à d'autres organismes d'application de la loi au Canada – tout renseignement biométrique et les renseignements personnels qui y sont associés à des fins d'établissement ou de contrôle de l'identité s'il s'agit de prévenir, d'instruire ou de réprimer une infraction¹²¹. Cette

¹¹⁵ L'alinéa 150.1(1) b) de la LIPR autorise le ministre à prendre des règlements concernant la communication de renseignements « en matière de sécurité nationale, de défense du Canada ou de conduite des affaires internationales ».

¹¹⁶ RIPR, partie 19,1, section 1.

¹¹⁷ RIPR, partie 19,1, section 3.

¹¹⁸ Voir en particulier la section 1, article 315.22 à 315,25; section 3, article 315.37 à 315,39.

¹¹⁹ Section 1, article 315.25(4), 315.26 et 315.27; section 3, article 315.41(3), 315.42 et 315.43.

¹²⁰ Réponse écrite d'IRCC à l'OSSNR, 20 novembre 2020, p. 13.

¹²¹ Alinéa 13.11(1)a) du RIPR; réponse écrite de la GRC à l'OSSNR, 31 mai 2021, p. 5. Voir aussi l'alinéa 150,1(1)d) de la LIPR qui autorise le ministre à prendre des règlements concernant « la conservation, l'utilisation, le retrait et la communication par la Gendarmerie royale du Canada de renseignements biométriques et des renseignements personnels y étant associés, qui sont recueillis sous le régime de la présente loi et qui lui sont communiqués pour le contrôle d'application des lois fédérales ou provinciales ». Le RIPR ne réglemente pas actuellement la conservation et le retrait des

information peut également servir à établir ou à contrôler une identité qui ne peut raisonnablement être établie ou vérifiée autrement en raison de tout état physique ou mental d'une personne ou de son décès¹²². En d'autres termes, lorsque les organismes d'application de la loi présentent à la GRC des empreintes digitales prises dans l'exercice de leurs fonctions – ou s'il s'agit pour la Gendarmerie royale de vérifier des empreintes digitales –, les répertoires tant de la criminalité que de l'immigration qui renferment les empreintes digitales des étrangers et des résidents permanents sont interrogés dans le cadre de cette recherche¹²³. Le paragraphe 13.11(2) du RIPR permet d'utiliser ou de communiquer les renseignements personnels suivants : empreintes digitales de l'intéressé et date de leur prise, nom de famille et prénom, autres noms et pseudonymes le cas échéant, date de naissance, sexe et numéro de tout dossier relatif aux renseignements biométriques ou aux renseignements personnels qui y sont associés.

Évaluation du Programme d'Immigration

86. La biométrie facilite la gestion de l'identité dans le cadre du Programme d'immigration. Premièrement, l'inscription des données biométriques permet de faire le lien entre une demande et une personne. Deuxièmement, la recherche biométrique permet de contrôler les demandeurs dans les bases de données nationales et étrangères, auquel cas les renseignements renvoyés par la suite éclairent les décisions d'admissibilité au Canada. Troisièmement, on vérifie les données biométriques à l'arrivée à un point d'entrée au Canada en voulant s'assurer que la personne qui se présente est bien celle à qui un visa ou un permis a été octroyé. Enfin, les données biométriques sont conservées pour une période déterminée (qui varie selon les catégories de demandes), de sorte qu'on puisse juger du maintien de l'admissibilité (statut) en vertu de la LIPR, tout en permettant aux étrangers de présenter ultérieurement des demandes sans avoir à réinscrire leurs données biométriques¹²⁴.
87. Les avantages en matière de sécurité nationale sont le fruit d'une solide gestion de l'identité. Cette sécurité est un élément parmi d'autres qui justifie le recours à la biométrie. L'inscription biométrique au stade de la demande peut avoir un effet dissuasif sur les gens qui autrement pourraient présenter une demande de mauvaise foi. Le contrôle biométrique dans les bases de données nationales et étrangères aide à repérer les gens interdits de territoire (entre autres pour

empreintes digitales prises par IRCC dans l'exercice de ses fonctions; voir plutôt l'analyse des politiques et des exigences de conservation de la *Loi sur la Bibliothèque et les Archives du Canada* au paragraphe 78.

¹²² RIPR, alinéa 13.11(1)b).

¹²³ Cela comprend les empreintes digitales latentes recueillies dans le cadre d'enquêtes criminelles. Réponse écrite de la GRC à l'OSSNR, 22 juin 2021, p. 9. Réponse écrite de la GRC à l'OSSNR, 1^{er} octobre 2021.

¹²⁴ Les demandes de résidence temporaire sont traitées en vertu de la politique « 1 en 10 », ce qui signifie que les données biométriques valent pour dix ans et peuvent être réutilisées (notamment à des fins de contrôle et de vérification) si des demandes sont présentées à nouveau ou ultérieurement dans ce laps de temps. En revanche, les demandes de résidence permanente nécessitent une collecte et une inscription biométrique pour chacune.

des raisons de sécurité nationale). En vérifiant les données biométriques à l'arrivée, on s'assure que la personne qu'on autorise à entrer – et non quelqu'un qui se fait passer pour l'intéressé – est bien celle qui entre au pays. La conservation des données biométriques – qui comprend la conservation dans le cas des demandes refusées pour des raisons de sécurité nationale – permet une évaluation continue de l'admissibilité en vertu de la LIPR (au regard notamment de l'article 34) et vient faciliter l'interrogation correspondante des bases de données étrangères. Sans la biométrie, les échanges reposeraient uniquement sur des renseignements biographiques se prêtant davantage à la fraude ou à l'erreur¹²⁵.

88. Étant propres à chacun et faciles à consigner au moyen de la technologie numérique, les empreintes digitales sont généralement considérées comme un moyen d'identification fidèle et sûr¹²⁶. Cependant, tant l'ASFC qu'IRCC ont soulevé d'éventuelles préoccupations sur le plan de l'analyse comparative entre les sexes plus (ACS+), laquelle est un processus analytique visant à évaluer les incidences des politiques, des programmes et des initiatives sur les divers groupes¹²⁷. Plus précisément, la prise des empreintes digitales est plus difficile pour certains groupes. Tel est le cas notamment des gens appartenant à certains métiers (ce qui pourrait indiquer une situation socioéconomique inférieure) et des femmes (en raison d'une différence biologique dans les crêtes des doigts)¹²⁸. Les stratégies d'atténuation au stade de la collecte comportaient une formation des préposés, des consignes opérationnelles et une disposition réglementaire (article 12.8 du RIPR) qui permet de poursuivre l'examen d'une demande si la prise des empreintes digitales est impossible¹²⁹.
89. De même, la recherche a montré que les algorithmes de correspondance dactyloscopique – comme ceux qui sont utilisés pour la vérification systématique des empreintes digitales – peuvent être moins précis pour certains groupes (ethnique, sexe, âge ou situation socioéconomique)¹³⁰. Des exemples en sont les gens d'origine est-asiatique, les femmes, les

¹²⁵ CIC et ASFC, « PIA - Canada-U.S. Systematic Biometric Information Sharing », p. 11 [IRCC DR n° 2 Documents].

¹²⁶ Les forces de l'ordre utilisent les empreintes digitales depuis le XIX^e siècle. La dactyloscopie n'a cependant rien d'infaillible; voir, par exemple, Jennifer Mnookin et coll. « Error rates for latent fingerprinting as a function of visual complexity and cognitive difficulty », mai 2016. Consultation le 1^{er} août 2021. <https://www.ojp.gov/pdffiles1/nij/grants/249890.pdf>.

¹²⁷ Pour plus de détails sur l'ACS+, voir gouvernement du Canada, « Qu'est-ce que l'Analyse comparative entre les sexes plus? », 14 avril 2021. Consultation le 30 août 2021. <https://femmes-egalite-genres.canada.ca/fr/analyse-comparative-entre-sexes-plus/est-analyse-comparative-entre-sexes-plus.html>.

¹²⁸ IRCC, « Triage – Biometrics Expansion – March 2017 », p. 3 [IRCC DR n° 2 Documents].

¹²⁹ Là où les conditions empêchant la collecte de données biométriques sont temporaires, les demandeurs peuvent être tenus de les fournir à une date ultérieure. S'il s'agit de conditions permanentes, les exigences biométriques peuvent être levées. Pour des exemples de blessures et d'états de santé qui nuisent à la prise biométrique et pour des instructions générales sur ces états dans le contexte des demandes d'immigration, voir gouvernement du Canada, « États de santé qui nuisent à la collecte des données biométriques », 30 juillet 2018. Consultation le 2 août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/publications-guides/bulletins-guides-operationnels/gestion-identite/biometriques/etat-sante.html>.

¹³⁰ P. Drozdowski et coll., « Demographic Bias in Biometrics : A Survey on an Emerging Challenge », 14 avril 2020. Consultation le 1^{er} août 2021. <https://arxiv.org/pdf/2003.02488>. Voir aussi R. Austin Hicklin et Christopher L. Reedy,

travailleurs de certains métiers et les personnes âgées. Ces groupes s'exposeraient à des taux d'erreur supérieurs lorsque leurs empreintes digitales sont vérifiées (comparées dans une base de données de renseignements dactyloscopiques)¹³¹. Au nombre des stratégies d'atténuation définies par l'ASFC, mentionnons les rajustements matériels et logiciels pouvant rendre les bornes d'inspection primaire (servant à la VSED) plus en mesure de prendre et d'analyser les empreintes digitales¹³².

90. En matière de transparence, le public a accès à beaucoup de renseignements sur la biométrie et le processus de demande d'immigration. Ce contenu est le plus souvent pratique, visant à guider les demandeurs éventuels dans la fourniture de leurs renseignements biométriques¹³³. IRCC explique par ailleurs les avantages du recours à la biométrie en faisant notamment valoir qu'elle facilite l'entrée au Canada, qu'elle garantit que la personne qui cherche à entrer est celle qui s'est vu accorder un visa, un permis ou la résidence permanente et qu'elle aide à prévenir l'introduction au pays de visas ou de permis volés, empruntés ou altérés¹³⁴. Des justifications fondées sur la sécurité nationale sont avancées, mais l'accent est mis sur la prestation des services et les impératifs plus larges de gestion de l'identité.
91. Somme toute, les empreintes digitales semblent être un choix biométrique raisonnable et approprié dans le système d'immigration. Elles peuvent être consignées avec une facilité relative sans guère d'intrusion et, bien que fiables comme identificateur, elles donnent relativement peu d'indices en soi sur le mode de vie ou les choix personnels des gens. De plus, elles assurent une interopérabilité essentielle entre les systèmes nationaux d'immigration et d'exécution de la loi et avec les systèmes de presque toutes les administrations étrangères. Les coûts en protection de la vie privée qui sont liés à la biométrie du contrôle de l'immigration paraissent donc raisonnables et proportionnés aux avantages pour l'État et l'intégrité du système d'immigration.
92. Une fois les données biométriques recueillies, leur utilisation à des fins de contrôle et de vérification s'inscrit dans l'objectif de gestion de l'identité. Du point de vue de la sécurité nationale, les décisions en matière d'admissibilité – sur qui peut ou non entrer au pays – sont fondamentales. Le sera tout autant le désir de prévenir l'accès frauduleux au territoire. À l'étape

« Implications of the IDENT/IAFIS Image Quality Study for Visa Fingerprint Processing », 31 octobre 2002. Consultation le 1^{er} août 2021. https://www.eumonitor.nl/9353000/1/j4nvgs5kig27kof_j9vvik7m1c3gyxp/vjf4n9jouqzh/f=/blg266612.pdf.

¹³¹ Hicklin et Reedy, « Implications of the IDENT/IAFIS Image Quality ».

¹³² ASFC, « Gender-Based Analysis Plus and the Primary Inspection Kiosk: Summary of Key Findings », mai 2016, p. 3 [OSSNR_202002_03_012, p. 3].

¹³³ Les renseignements visent notamment à répondre aux questions suivantes : en quoi la biométrie consiste-t-elle? quels renseignements biométriques sont recueillis? de qui ces renseignements sont-ils obtenus (et qui en est exempté)? comment la collecte et la vérification des données biométriques fonctionnent-elles? où et comment inscrire ses données biométriques? combien le processus coûte-t-il (tarification)? comment la vie privée est-elle protégée? Cette information offre des réponses à des questions fréquemment posées. Voir ASFC, « Contrôle biométrique », 12 août 2020. Consultation le 1^{er} août 2021. <https://www.cbsa-asfc.gc.ca/security-securite/biometrics-biometrique-fra.html>; IRCC, « Expansion de la biométrie », 4 février 2019. Consultation le 1^{er} août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/campagnes/biometrie.html>.

¹³⁴ IRCC, « Pourquoi dois-je fournir mes données biométriques (empreintes digitales et photo) lorsque je présente une demande? » 29 septembre 2021. Consultation le 5 octobre 2021. <https://www.cic.gc.ca/francais/centre-aide/reponse.asp?qnum=703&top=19>.

du contrôle, la biométrie est particulièrement utile pour établir des liens entre les renseignements des différentes bases de données, par exemple à faire le lien entre les renseignements sur une personne dans les répertoires nationaux ou étrangers. La capacité d'établir de tels liens même en présence d'une pluralité de noms ou de profils biographiques – peut-être employés de mauvaise foi – est en grande partie une caractéristique propre aux données biométriques. De même, la vérification, c'est-à-dire la confirmation qu'une personne est bien celle qu'elle prétend être lorsqu'elle se présente à la frontière, est largement améliorée par l'analyse biométrique.

93. Les activités ne sont néanmoins pas sans risques. Par exemple, parce que les données biométriques de l'immigration sont à la disposition des organismes canadiens d'application de la loi, il existe un risque que les immigrants soient stigmatisés en raison de leur association avec la criminalité. En 2015, EURODAC (base européenne de données dactyloscopiques pour les demandes d'asile) de l'Union européenne a abondamment été critiquée par les groupes de défense des droits civils pour « avoir criminalisé » les demandeurs d'asile en mettant leurs fiches dactyloscopiques à la disposition des organismes européens d'application de la loi¹³⁵. Bien que tenues dans des répertoires distincts, les données dactyloscopiques de l'immigration et de la criminalité existent dans le même système de la GRC et les unes et les autres sont consultables par les organismes d'application de la loi, notamment lorsqu'ils veulent analyser les empreintes digitales inconnues prélevées sur les lieux du crime¹³⁶.
94. Il y a des avantages à mettre les données dactyloscopiques de l'immigration à la disposition des forces de l'ordre, premièrement pour aider la police dans son application du droit pénal au Canada, et il est avantageux de communiquer ces données à IRCC et à l'ASFC si elles peuvent servir à l'application de la LIPR. Il faut cependant avouer que, si les empreintes digitales de tous les citoyens canadiens étaient en la possession du gouvernement et consultables par les forces de l'ordre, il y aurait encore là un avantage pour l'application de la loi au pays, mais peu de gens – s'il en est – jugeraient une telle mesure pertinente ou souhaitable. Il est donc légitime de se demander si la disponibilité des données dactyloscopiques de l'immigration – information recueillie à l'occasion des demandes d'entrée en territoire canadien – pour les organismes d'application de la loi est pertinente dans toutes les circonstances ou si elle devrait se limiter aux cas d'infractions graves.

¹³⁵ Sergio Carrera et coll., « When mobility is not a choice : Problematising asylum seekers' secondary movements and their criminalization in the EU », CEPS, décembre 2019. Consultation le 1^{er} août 2021. <https://www.ceps.eu/wp-content/uploads/2019/12/LSE2019-11-RESOMA-Policing-secondary-movements-in-the-EU.pdf>. Voir aussi Andrea Dernbach (traduction d'Erika Korner), « Eurodac fingerprint database under fire by human rights activists », *Euractiv*, 9 février 2016. Consultation le 1^{er} août 2021. <https://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/>.

¹³⁶ Si les données dactyloscopiques de l'immigration ne sont pas comparées aux empreintes digitales inconnues au moment de l'inscription, les empreintes inconnues recueillies dans le cadre d'enquêtes criminelles peuvent être comparées dans les dépôts de données dactyloscopiques de l'immigration. Réponse écrite de la GRC à l'OSSNR, 1^{er} octobre 2021.

Programme de passeport

95. Le Programme de passeport, dirigé par IRCC, « s'occupe de délivrer, de refuser de délivrer, de révoquer, de conserver, d'annuler et de récupérer les passeports et autres documents de voyage canadiens, en plus de fournir des instructions sur leur utilisation¹³⁷ ». Son but ultime est de permettre aux citoyens, aux résidents permanents et aux réfugiés au pays de voyager s'ils sont admissibles. Ainsi, le programme de passeport permet d'empêcher les gens inadmissibles ou n'ayant pas droit à un passeport d'en obtenir un et de voyager avec des documents officiels. Certains demandeurs seront inadmissibles pour cause de sécurité nationale. Pris conformément à la prérogative royale sur les passeports, le Décret sur les passeports canadiens (DPC) constitue le principal cadre juridique pour la délivrance de passeports ordinaires et temporaires dans le cadre de ce programme¹³⁸. Il habilite IRCC à recueillir et à utiliser des renseignements personnels, y compris des données biométriques, pour le traitement des demandes et la détermination du droit d'une personne à un passeport¹³⁹. IRCC soutient que cette collecte est conforme à l'article 4 de la *Loi sur la protection des renseignements personnels*, car elle a directement à voir avec l'administration d'un programme dûment autorisé¹⁴⁰.
96. Plus précisément en ce qui concerne la biométrie, le paragraphe 8.1(1) du DPC permet à IRCC de convertir la photo d'un demandeur en format numérique et de l'insérer sur la puce dans le

¹³⁷ IRCC, « Évaluation du Programme de passeport », mars 2020. Consultation le 18 août 2021.

<https://www.canada.ca/fr/immigration-refugiees-citoyennete/organisation/rapports-statistiques/evaluations/evaluation-du-programme-de-passeport.html>, p. 6. L'annulation et la révocation sont deux processus administratifs distincts en réaction à des situations différentes. Les décisions de *révocation* sont considérées définitives à la date à laquelle elles sont rendues et elles font suite à une enquête détaillée où la personne en cause a la possibilité de répondre avant de recevoir la décision. Cela comprend les cas où le ministre de la Sécurité publique et de la Protection civile a « des motifs raisonnables de croire que cela [la décision] est nécessaire pour prévenir la commission d'une infraction de terrorisme, au sens de l'article 2 du *Code criminel*, ou pour la sécurité nationale du Canada ou d'un pays ou État étranger » (voir le DPC, article 10.1). Quelqu'un peut demander par écrit la révision d'une décision d'*annulation* de passeport dans les 30 jours suivant la date à laquelle il apprend l'annulation (voir l'article 11.3 du DPC et, pour la possibilité de réexamen, l'article 11.31). Dans les deux cas, les agents d'application de la loi et de contrôle frontalier sont avisés de l'annulation ou de la révocation et le passeport ne peut plus être utilisé dans le cadre d'un voyage. Voir aussi IRCC, <https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens/securite-passeports/refus-revocation.html>.

¹³⁸ Voir tout le texte à <https://laws.justice.gc.ca/fra/reglements/TR-81-86/>.

¹³⁹ Le DPC autorise ces activités en ce qui concerne les passeports ordinaires (bleus) et temporaires (blancs). Pour les autres documents de voyage officiels, qu'il s'agisse de passeports spéciaux (verts) et diplomatiques (rouges), de certificats d'identité, de documents de voyage pour réfugiés ou de documents de voyage d'urgence, la décision est prise par le ministre de l'Immigration, des Réfugiés et de la Citoyenneté qui exerce la prérogative royale. Celle-ci s'applique aux activités non explicitement autorisées par la loi, mais qui ont de tout temps été exercées par le pouvoir exécutif.

¹⁴⁰ De même, le DPC confère au ministre de l'Emploi et du Développement social (article 12), par l'entremise de Service Canada, et au ministre des Affaires étrangères (article 13), par l'entremise d'Affaires mondiales Canada, le pouvoir de recueillir des renseignements personnels dans le cadre du processus de demande. C'est en vertu de la même prérogative royale qu'AMC est habilité à recevoir et à traiter les demandes de documents de voyage d'urgence.

passport électronique. Le paragraphe 8.1(2) facilite l'utilisation du système de reconnaissance faciale en autorisant la conversion de la photo du demandeur en un modèle biométrique « pour vérifier son identité – y compris sa nationalité – et son admissibilité à obtenir un passeport ou à le garder en sa possession¹⁴¹ ». Ces dispositions autorisent de même l'utilisation de la liste des signalements du Système de reconnaissance faciale (LS-SRF) que nous allons décrire.

97. Comme pour le Programme d'immigration, les avantages du recours à la biométrie vont dans leur ensemble au-delà des résultats en matière de sécurité nationale. D'après IRCC, [traduction] « le recours à la biométrie dans le Programme de passeport ne constitue pas en soi une activité relevant de la sécurité et du renseignement¹⁴² ». Comme dans le Programme d'immigration, il sert plutôt à la gestion de l'identité en pouvant apporter, plus particulièrement en aval de cette démarche plus large, des avantages en matière de sécurité nationale.
98. Deux photos du visage imprimées à l'identique et conformes à certaines normes de l'Organisation de l'aviation civile internationale (OACI) doivent être présentées avec les demandes de documents de voyage canadiens¹⁴³. Selon IRCC, tous les renseignements des demandes sont transmis par des voies sécurisées et toute la circulation de données de reconnaissance faciale est protégée par chiffrement¹⁴⁴.
99. La photo prise sert à deux fins. D'abord, elle est contrôlée par reconnaissance faciale à des fins d'établissement de l'identité et fournit des indications pour l'évaluation de l'admissibilité du demandeur et de son droit aux services des documents de voyage canadiens¹⁴⁵. Ensuite, elle est intégrée au document et les agents des services frontaliers s'en servent pour valider l'identité du titulaire lorsqu'il traverse une frontière internationale.
100. La photo numérisée du demandeur est transmise à l'application Solution de reconnaissance faciale (SRF). La SRF convertit l'image en modèle biométrique à l'aide d'un algorithme propre et la verse dans une base de données connexe. Si la demande est liée à une demande antérieure, par exemple de renouvellement ou de remplacement d'un passeport perdu ou volé, une comparaison faciale individuelle se fait avec le ou les modèles biométriques antérieurs du demandeur. Tant pour les renouvellements que pour les nouvelles demandes, on procède à une identification faciale collective par rapport aux modèles existants (on en compte approximativement 55 millions liés aux demandes antérieures) dans la base de données SRF en provenance de demandeurs adultes (âgés de 16 ans et plus), sans oublier les photos fournies dans le cadre de la liste des signalements (LS) du système des passeports. La LS-SRF comme on l'appelle est en fait une liste d'avis de surveillance où figurent les gens considérés comme représentant un risque élevé de fraude d'identité, ce qui comprend les gens connus pour avoir utilisé de fausses identités ou plusieurs pseudonymes ou qui ont autrement été désignés par les partenaires de sécurité – comme le SCRS et la GRC – comme présentant un risque élevé pour de

¹⁴¹ DPC, paragraphe 8.1(2).

¹⁴² Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 1.

¹⁴³ Les lignes directrices applicables précisent la taille, la disposition, les conditions d'éclairage, l'arrière-plan et l'expression faciale. Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 4.

¹⁴⁴ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 6.

¹⁴⁵ Les demandeurs de moins de 16 ans n'ont pas leur photo contrôlée par reconnaissance faciale, en raison des problèmes connus de précision de la correspondance faciale dans le cas des enfants.

tels agissements¹⁴⁶. Les critères ou circonstances précis d'inscription sur cette liste ne sont pas clairs et semblent hautement discrétionnaires¹⁴⁷. Cependant, IRCC apporte une précision : [traduction] « Seul un petit nombre d'agents du Programme de passeport d'IRCC peuvent ajouter des entrées à la liste¹⁴⁸. » La liste des signalements est en vigueur depuis février 2018 et comprend actuellement moins d'une centaine de personnes¹⁴⁹.

101. Selon IRCC, l'application de la SRF protège l'intégrité du passeport canadien. IRCC cite les lignes directrices de 2016 de l'OACI sur la sécurité de la délivrance de documents de voyage en mentionnant que l'étape de la délivrance – ou le [traduction] « début de la chaîne » – devient la cible préférée des fraudeurs, si on considère [traduction] « l'évolution rapide des nouvelles technologies et des nouvelles techniques en matière de sécurité », ce qui rend la contrefaçon de plus en plus difficile, dans le cas des caractéristiques de sécurité liées au passeport électronique, par exemple¹⁵⁰.
102. Le pouvoir de refuser les demandes de passeport pour des raisons de sécurité nationale revient au ministre de la Sécurité publique en vertu du Décret sur les passeports canadiens (DPC)¹⁵¹. Le contrôle biométrique par la SRF peut éclairer la prise de décisions, car il permet de détecter les cas de fraudes d'identité ou les signalements dans le cadre de la LS-SRF. Aucune décision n'est automatique; les gens signalés par ce moyen pourraient toujours, après examen de leur cas, avoir droit à un passeport ou à un document de voyage.
103. La prévention de la fraude (par dissuasion ou détection) pour la délivrance de documents de voyage officiels offre de nets avantages du point de vue de la sécurité nationale. Le passage de gens de mauvaise foi à la frontière menace la sécurité tant internationale que nationale au Canada. La fraude d'identité est commise pour une foule de raisons – notamment à des fins criminelles, financières ou personnelles –, mais on connaît bien la possibilité que l'utilisation frauduleuse de passeports joue un rôle dans le terrorisme, l'espionnage ou les autres menaces à

¹⁴⁶ Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 1 et 6.

¹⁴⁷ Parmi les exemples hypothétiques présentés à l'OSSNR à la séance d'information du 14 octobre 2020, il y a le cas d'un partenaire de sécurité, [traduction] « habituellement la GRC », indiquant qu'une personne inadmissible à un passeport peut tenter de présenter une demande sous un autre nom ou que des [traduction] « courtiers » achetaient des pièces d'identité dans certains milieux pour faciliter l'acquisition de documents de voyage par des personnes inadmissibles. Dans une réponse écrite à l'OSSNR le 1^{er} octobre 2021, IRCC a annoncé ce qui suit : [traduction] « Le Programme de passeport revoit actuellement la liste des signalements (LS) en vue de mieux documenter son objet, sa forme et son utilisation, de clairement indiquer les rôles et les responsabilités des intervenants et d'examiner le respect des paramètres législatifs et réglementaires applicables du Ministère. L'intervenant responsable s'occupera de tout point à améliorer constaté dans la fonctionnalité, l'efficacité ou les procédures opérationnelles. »

¹⁴⁸ Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 8.

¹⁴⁹ Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 8.

¹⁵⁰ OACI, « ICAO Guide for Assessing Security of Handling and Issuance of Travel Document », 2016. Consultation le 4 août 2021, p. 3. Disponible à <https://www.icao.int/security/fal/trip/pages/publications.aspx>.

¹⁵¹ Voir DPC, article 10.1, paragraphe 11.1(2) et article 11.4 (par lesquels le ministre de la Citoyenneté et de l'Immigration appuie le ministre de la Sécurité publique et de la Protection civile en donnant effet à ses décisions).

la sécurité nationale¹⁵². Rappelons que même si un événement est rare, cela ne signifie pas qu'il n'a pas de conséquences graves.

104. Un autre usage fondamental des données biométriques recueillies est le passeport électronique même¹⁵³ pendant un voyage à l'étranger. Quand le passeport est délivré, la photo faciale est à la fois imprimée sur la page biographique et intégrée comme image numérique à une puce électronique dans le document¹⁵⁴.
105. La photo numérique intégrée permet une triple vérification entre l'image sur le passeport, l'image sur la puce et la personne qui présente le passeport. Certains pays – dont le Canada (voir l'analyse des bornes d'inspection primaire aux paragraphes 125 à 137 plus loin) – tirent parti de la technologie de reconnaissance faciale à cette fin. Il en résulte une plus grande assurance a) quant à l'intégrité et à l'authenticité du document et b) quant à la vérification d'identité de la personne qui présente celui-ci. La puce comporte une signature numérique grâce aux techniques d'infrastructure à clé publique (ICP), ce qui permet de vérifier le document par rapport au pays de délivrance et de s'assurer que les données que renferme la puce n'ont pas été modifiées¹⁵⁵.
106. Les photos présentées dans une demande de passeport et les modèles biométriques qui en sont tirés sont conservés jusqu'à ce que le demandeur ait atteint l'âge de 100 ans¹⁵⁶. IRCC considère que cette durée de conservation est conforme aux pratiques des partenaires internationaux (entre autres le Royaume-Uni et l'Australie¹⁵⁷). Elle représente, selon lui, un juste

¹⁵² Voir, par exemple, Martin Rudner, « Misuse of Passport : Identity Fraud, the Propensity to Travel, and International Terrorism », *Studies in Conflict & Terrorism*. 2008, 31 (2) : 95 à 110; Stefano Musco et Valter Coralluzzo, « Sneaking Under Cover : Assessing the Relevance of Passport for Intelligence Operations », 2016. *International Journal of Intelligence and Counter Intelligence*. 2016. 29 (3) : 427 à 446.

¹⁵³ Comme il est indiqué à la section IV, le passeport électronique a été implanté au Canada en 2013. Il s'agit aujourd'hui d'un document reconnu sur le plan international qui est délivré dans plus de 135 pays et régi par les spécifications de l'OACI.

¹⁵⁴ La photo du visage est obligatoire pour le passeport électronique selon les lignes directrices de l'OACI. Voir OACI, « Doc 9303 : « Documents de voyage lisibles à la machine », huitième édition, 2021. Consultation le 4 août 2021. https://www.icao.int/publications/Documents/9303_p9_cons_fr.pdf. Ces lignes directrices permettent aussi la lecture de l'iris et la dactyloscopie comme modes biométriques facultatifs, mais le Canada ne recueille pas de telles données et celles-ci ne figurent pas non plus dans la version canadienne du passeport électronique. Au moment de la mise en place de ce passeport en 2013, Passeport Canada n'avait pas exprimé l'intention de recueillir des empreintes rétiniennes, des empreintes digitales ou tout autre renseignement biométrique dans le cadre de ce programme. Il a reconnu que des modifications réglementaires ou de nouvelles évaluations des facteurs relatifs à la vie privée seraient nécessaires avant que des mesures ne soient adoptées en ce sens. Passeport Canada, « PIA National Rollout of ePassport 2013 », p. 112 [IRCC DR n° 2 Documents].

¹⁵⁵ Le processus est décrit dans OACI, « Basics of ePassport Cryptography », sans date, consultation le 20 août 2021. <https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Basics.aspx>

¹⁵⁶ Si quelqu'un est titulaire d'un passeport canadien valide qui expirera après son 100^e anniversaire, la demande de passeport et les documents à l'appui sont conservés sur support électronique pendant une période supplémentaire correspondant à la période de validité du passeport. Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2021, p. 6.

¹⁵⁷ Passeport Canada, « PIA National Deployment of ePassport 2013 », p. 121 [IRCC DR n° 2 Documents].

équilibre entre la nécessité de délivrer des documents de voyage sécurisés et inspirant la confiance, d'une part, et l'obligation en vertu de la *Loi sur la protection des renseignements personnels* de conserver les renseignements personnels uniquement aussi longtemps qu'il est nécessaire sans plus, d'autre part¹⁵⁸. Les copies papier des demandes de passeport avec les photos sont conservées pendant six semaines après la conversion au format numérique, puis déchiquetées.

107. La période de conservation facilite la gestion de l'identité si on considère que les gens sont appelés à renouveler leur passeport au cours de leur vie. Chaque adulte auteur d'une nouvelle demande (renouvellement, remplacement, etc.) peut faire l'objet d'une vérification au moyen de la SRF par rapport à ses demandes antérieures. De même, une identification SRF collective fait intervenir les modèles de la plupart des demandeurs adultes, d'où une possibilité maximale de détecter les fraudes d'identité possibles.
108. IRCC communique aux autres ministères (AM) les photos et autres renseignements biographiques recueillis par le Programme de passeport. Contrairement à la situation dans le Programme d'immigration, la communication n'est pas systématique. Elle se fait plutôt sur *demande ponctuelle* des autres ministères ayant un mandat en matière de criminalité, de sécurité nationale ou de renseignement. Les AM produisent leurs demandes en vertu de leurs propres lois et l'applicabilité en est circonscrite par l'article 4 de la *Loi sur la protection des renseignements personnels*¹⁵⁹. Selon IRCC, nombre de ces demandes ont souvent pour contexte le besoin de renseignements sur les Canadiens qui se déplacent à l'étranger pour participer à des conflits ou à des actes illicites¹⁶⁰.
109. Il peut s'agir de demandes de confirmation ou de validation de renseignements biométriques fournis par d'autres ministères par rapport aux dossiers des passeports ou encore d'identification de personnes préoccupantes pour la sécurité par le traitement d'une photo fournie par les AM dans le cadre de la SRF¹⁶¹. Ainsi, la GRC peut identifier une personne qui présente un risque pour la sécurité nationale en ayant seulement une photo de l'intéressé (du fait de sa présence dans les médias sociaux, par exemple); le SCRS peut communiquer à IRCC la photo d'une personne sur qui il fait enquête, mais sans pouvoir en établir l'identité. Autre possibilité, la GRC et le SCRS peuvent échanger avec IRCC des photos d'individus connus. Le but de ces contrôles est de s'assurer que personne n'obtient de passeport sous une autre identité que la sienne¹⁶². IRCC affirme que, dans le cas de la GRC, les scénarios décrits peuvent exiger que celle-ci obtienne une ordonnance de communication selon les circonstances particulières de la demande.
110. Dans les deux cas, IRCC convertit la photo fournie par le SCRS ou la GRC en modèle biométrique et la soumet au SRF. Dans le premier cas, IRCC renvoie, en cas de correspondance, des renseignements biographiques ou biométriques limités à la GRC ou au SCRS pour l'aider à

¹⁵⁸ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 6.

¹⁵⁹ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 9 et 12; voir, par exemple, l'article 12 et le paragraphe 19(2) de la Loi sur le SCRS, L.R.C. 1985, ch. C-23, ainsi que l'alinéa 18a) de la *Loi sur la GRC*, L.R.C. 1985, ch. R-10.

¹⁶⁰ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 9.

¹⁶¹ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 9.

¹⁶² Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 9.

confirmer l'identité de l'intéressé. Dans le second, IRCC peut valider l'identité déjà connue de la personne et confirmer si sa photo est rattachable à toute autre identité enregistrée par le Programme de passeport. Dans l'un et l'autre des cas, la portée des renseignements communiqués par IRCC dépend de la nature de l'enquête et de ses pouvoirs de communication¹⁶³.

111. IRCC communique cette information conformément à l'article 5 de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), le cas échéant, ou il peut invoquer l'alinéa 8(2)e) de la *Loi sur la protection des renseignements personnels* dans le cas de demandes particulières¹⁶⁴. L'article 5 de la LCISC lui permet de communiquer des renseignements à la GRC, au SCRS et à d'autres institutions désignées¹⁶⁵ s'il a la conviction que cette communication contribuera à l'exercice de la compétence de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité du Canada. La LCISC exige que l'incidence de cette communication sur le droit à la vie privée se limite à ce qui est raisonnablement nécessaire dans les circonstances¹⁶⁶. IRCC affirme que, lorsqu'il envisage une communication, il obtient d'abord suffisamment de détails pour s'assurer que les conditions sont respectées¹⁶⁷. Dans d'autres cas, s'il s'agit, par exemple, d'une communication devant faciliter une enquête d'exécution de la loi, il peut se fonder sur l'alinéa 8(2)e) de la *Loi sur la protection des renseignements personnels* pour fournir à des organismes d'enquête particuliers¹⁶⁸ les renseignements qu'ils ont demandés par écrit aux fins de l'application des lois canadiennes ou de la tenue d'une enquête légale¹⁶⁹. Si une ordonnance de communication ou un mandat accompagne les demandes d'autres ministères, l'alinéa 8(2)c) de la *Loi sur la protection des renseignements personnels* autorise la communication de renseignements en conformité avec l'ordonnance ou le mandat.

112. La communication de tels renseignements ne se limite pas aux fins de la sécurité nationale ou des enquêtes d'exécution de la loi, puisque IRCC peut communiquer au besoin des

¹⁶³ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 9.

¹⁶⁴ Réponse écrite d'IRCC à l'OSSNR, 4 décembre, p. 12. Voir aussi *Loi sur la communication d'information ayant trait à la sécurité du Canada*, L.C. 2015, ch. 20, articles 2 et 5; *Loi sur la protection des renseignements personnels*, L.R.C., 1985, ch. P-21, alinéa 8(2)e).

¹⁶⁵ Voir la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, L.C. 2015, ch. 20, article 2, paragraphe 5(1) et annexe III. Les institutions destinataires admissibles comprennent l'ASFC, le CST et le ministère de la Sécurité publique et de la Protection civile.

¹⁶⁶ LCISC, *ibid.*, paragraphe 5(1).

¹⁶⁷ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 12. Voir aussi la LCISC et le document du CPVP intitulé « Review of Federal Institutions' Disclosures of Information Under the Security of Canada Information Disclosure Act in 2020 » au sujet des pratiques générales d'IRCC à cet égard.

¹⁶⁸ Ces organismes sont énumérés à l'annexe II du *Règlement sur la protection des renseignements personnels*, DORS/83-508 et comprennent le SCRS, la GRC et trois sous-groupes de l'ASFC, à savoir la Division de l'exécution de la loi dans les bureaux intérieurs, la Direction des opérations de ciblage et du renseignement et la Division des enquêtes criminelles.

¹⁶⁹ Réponse écrite d'IRCC à l'OSSNR, 4 décembre, p. 12; voir aussi l'alinéa 8(2)e) de la *Loi sur la protection des renseignements personnels*.

renseignements au ministère de la Sécurité publique en vue d'aider son ministre à rendre une décision en vertu du Décret sur les passeports canadiens. L'article 10.1 et le paragraphe 11.1(2) du Décret autorisent le ministre de la Sécurité publique à juger si un passeport ne devrait pas être délivré ou si un passeport en cours devrait être révoqué ou annulé afin d'empêcher la perpétration d'un acte terroriste ou de sauvegarder la sécurité nationale du Canada ou d'un État étranger¹⁷⁰. C'est en vertu de ce pouvoir qu'IRCC peut recueillir en permanence des renseignements permettant de vérifier si une personne a toujours le droit d'être titulaire d'un passeport¹⁷¹. IRCC s'appuie en outre sur le DPC pour communiquer au ministre de la Sécurité publique les renseignements nécessaires aux décisions à prendre sur ces questions¹⁷². Dans la pratique, cela comprend la communication par le Ministère de la demande de passeport avec la photo numérisée à Sécurité publique Canada¹⁷³. L'article 5 de la LCISC et l'alinéa 8(2)a) de la *Loi sur la protection des renseignements personnels* (usages compatibles) permettent également cette communication¹⁷⁴.

Évaluation du Programme de passeport

113. La possibilité d'erreurs associée à la technologie constitue une importante source de préoccupations du public en ce qui concerne le recours à la reconnaissance faciale. Dans le contexte des passeports, un faux positif en matière d'identité peut causer des inconvénients aux gens ou entraîner une enquête à leur endroit¹⁷⁵. En revanche, les faux négatifs préoccupent les utilisateurs de la technologie, car ils risquent de compromettre les avantages du système en matière de sécurité.
114. La SRF jouit de certains avantages naturels en fait d'exactitude. D'abord, elle utilise surtout les images captées de grande qualité (modèles extraits de photos de passeport prises selon les spécifications de l'OACI) et la comparaison se fait avec ces mêmes modèles (c'est une galerie de portraits modèles extraits des photos de passeport)¹⁷⁶. Les exceptions sont les images de la liste des signalements LS-SRF et les images fournies par les AM pour vérification par rapport aux

¹⁷⁰ CPVP, article 10.1 et paragraphe 11.1(2).

¹⁷¹ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 11.

¹⁷² Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 8. Voir aussi CPVP, article 11.4.

¹⁷³ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 8 et 9.

¹⁷⁴ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 12.

¹⁷⁵ Les résultats de la reconnaissance faciale ne peuvent entraîner automatiquement le refus de la demande, les décisions n'étant pas rendues d'après ces seuls résultats. Il reste que, si un faux positif n'est pas relevé ou corrigé, on peut penser que cet élément de preuve jouera grandement dans le rejet de la demande. Comme un faux positif non relevé ni corrigé ne serait pas considéré comme une erreur, il est impossible de recueillir des données sur de tels cas.

¹⁷⁶ Le NIST a déterminé que la qualité des images est un important facteur de réduction du biais introduit par les algorithmes de reconnaissance faciale. Voir NIST, « Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects », décembre 2019. Consultation le 5 août 2021. <https://doi.org/10.6028/NIST.IR.8280>

données de la SRF. Ces images risquent d'être d'une moindre qualité. Ensuite, le processus de comparaison n'est pas sensible au temps (comme dans le cadre concret des points d'entrée). Une analyse approfondie quant à la correspondance (identification collective) ou à l'absence de correspondance (vérification individuelle) – par triage, analyse et enquête – peut être menée avant que des décisions susceptibles d'affecter des personnes ne soient prises.

115. Une préoccupation connexe est que certains groupes seront touchés de façon disproportionnée par les inexactitudes du système. Des recherches expresses ont démontré que, entre autres facteurs, l'âge, le sexe et l'origine ethnique peuvent influencer la capacité d'un système de reconnaissance faciale à dûment reconnaître les gens, d'où des possibilités de biais et de discrimination¹⁷⁷.
116. IRCC recourt à plusieurs mesures d'atténuation. D'abord, les modèles inscrits sont classés dans une des six galeries selon l'âge (adultes de 16 ans et plus et enfants de moins de 16 ans) et le sexe autodéclaré (homme, femme ou autre). On sait que l'âge et le sexe sont des facteurs de confusion dans la reconnaissance faciale; la division de la base de données en galeries en fonction de telles caractéristiques permet d'adapter les seuils au besoin et d'ainsi améliorer le rendement du système.
117. En janvier 2021, IRCC a mené à terme l'évaluation d'un algorithme de nouvelle génération à utiliser dans le cadre de la SRF¹⁷⁸. Les résultats obtenus se sont révélés favorables en fait d'exactitude des tests, et la mise en œuvre du nouvel algorithme est prévue pour 2021-2022¹⁷⁹. Plus précisément, celui-ci s'est révélé d'un rendement supérieur sur le plan des différences selon l'âge et le sexe comparativement à l'algorithme en usage. Le nouvel algorithme a démontré un gain au chapitre de la mise en correspondance des photos prises à de longs intervalles (15 ans, par exemple), ce qui est directement utile pour les renouvellements de passeport. Les tests n'ont toutefois pas permis d'évaluer le rendement de l'algorithme pour ce qui est de la race et de l'origine ethnique.
118. IRCC informe le public sur le recours à la reconnaissance faciale dans le processus de demande de passeport. Les consignes relatives aux photos publiées sur le site Web d'IRCC indiquent : « L'Organisation de l'aviation civile internationale recommande une expression faciale neutre sur les photos de passeport. *Cela nous permet d'utiliser des systèmes de reconnaissance faciale pour aider à prévenir la fraude [...]*¹⁸⁰. » De même, un énoncé de confidentialité inclus dans les formulaires de demande de passeport décrit la collecte, l'utilisation, la communication et la conservation de renseignements personnels, y compris de données biométriques.
119. Les données biométriques intégrées à la puce du passeport électronique ne présentent pas de risque important ni ne vont au-delà de ce qui figurait dans les passeports analogiques avant l'avènement du passeport électronique. Ce qui figure sur la puce – image faciale et renseignements biographiques – figure aussi à la page 2 (biographique) de la version papier du document.

¹⁷⁷ NIST, « Face Recognition Vendor Test (FRVT) Part 3 ».

¹⁷⁸ IRCC, « IRCC Facial Recognition Algorithm Analyses 2021 » [IRCC DR n° 2 Documents].

¹⁷⁹ Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 4.

¹⁸⁰ Gouvernement du Canada, « Photos de passeport », 5 octobre 2010. Consultation le 5 août 2021.

<https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens/photos.html>. [Nous soulignons.]

120. En revanche, le processus de délivrance avec l'utilisation de la SRF fait directement intervenir tant les renseignements biométriques que les considérations de sécurité nationale. Empêcher les gens de mauvaise foi comme ceux qui menacent la sécurité nationale ou internationale d'obtenir des documents de voyage *authentiques* justifie des processus et des mesures de sécurité rigoureux à l'étape de la délivrance. Par ailleurs, l'information recueillie et utilisée dans le processus de délivrance touchera tous les gens c'est-à-dire les millions de Canadiens et d'autres personnes qui vivent au Canada qui sollicitent un passeport ou un autre document de voyage officiel.
121. La grande question est de savoir si l'avantage pour la sécurité nationale qui découle de la collecte, de l'utilisation, de la conservation et de la communication de renseignements biométriques justifie l'effet sur la vie privée de la SRF.
122. Il est bon de regarder dans ce contexte l'enquête récente du CPVP sur l'usage fait par la GRC des services de reconnaissance faciale fournis par l'entreprise privée Clearview-AI¹⁸¹. Dans ce cas, le Commissariat a conclu que l'exploitation que faisait la GRC de l'information recueillie par Clearview-AI dans les médias sociaux et à d'autres sources Internet allait à l'encontre de la *Loi sur la protection des renseignements personnels*, parce que la collecte des données en question par ce fournisseur avait été contraire à la loi. Plus proche de notre propos est cependant la caractérisation par le CPVP de l'*effet pratique* de l'utilisation de Clearview-AI dans le cadre de l'application de la loi, qui a fait en sorte que [traduction] « des milliards de personnes se sont retrouvées tous les jours, 24 heures sur 24, dans une parade d'identification policière¹⁸² ». En d'autres termes, l'existence des renseignements biométriques des gens dans une base de données à la disposition des organismes d'application de la loi signifiait que leur identification par les forces de l'ordre était possible en tout temps.
123. Dans le cas d'enquêtes sur la sécurité nationale, des justifications stratégiques, des avantages en matière de sécurité et des limites imposées à la communication peuvent rendre plus pertinente l'utilisation de la base de données des passeports d'IRCC. La communication de cette information à la GRC par le Ministère s'appuie aussi sur des pouvoirs conférés par la loi (voir le paragraphe 111). L'utilité des données biométriques des passeports dans le cadre des enquêtes et activités de la GRC, du SCRS et de l'ASFC demeure toutefois un exemple frappant de liens que permet d'établir la biométrie. À l'avenir, l'OSSNR pourrait souhaiter examiner de tels liens et juger de leur caractère raisonnable et nécessaire sous l'angle de l'équilibre à atteindre entre les intérêts individuels (vie privée, liberté, etc.) et les objectifs de l'État en matière de sécurité.

¹⁸¹ Commissariat à la protection de la vie privée, « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée ». À noter cependant que la GRC ne s'est jamais servie de Clearview-AI en relation avec le Programme d'immigration. Nous évoquons l'enquête du CPVP comme illustration de la nature des enjeux de confidentialité que peut poser la biométrie en général.

¹⁸² Commissariat à la protection de la vie privée, « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée ».

Arrivée au Canada

124. Le Programme de passeport et le Programme d'immigration sont les principaux programmes qui régissent le continuum frontalier canadien. Ensemble, ils aident à gérer les processus par lesquels les gens entrent au pays, surtout en produisant la documentation qui rend possibles les voyages à l'étranger. Est liée à ces programmes plus vastes le processus concret de l'arrivée à un point d'entrée et du passage par la douane et l'immigration canadiennes. Ce que nous avons dit de l'un et l'autre de ces programmes touchait à ce processus, et nous aborderons ici deux autres activités qui comportent une analyse de données biométriques à des fins de contrôle d'identité des gens qui arrivent au pays.

Bornes d'inspection primaire (BIP)

125. Les bornes d'inspection primaire (BIP) sont des bornes libre-service automatisées qui sont présentes dans dix grands aéroports canadiens¹⁸³. Elles facilitent le traitement à l'immigration et à la douane des arrivées internationales au Canada.
126. Comme nous l'avons mentionné à propos du Programme d'immigration, les étrangers ayant des données biométriques inscrites font l'objet d'une vérification biométrique à leur arrivée au Canada. Aux aéroports outillés pour la vérification systématique des empreintes digitales (VSED), cet examen se fait aux BIP¹⁸⁴. Ajoutons que ces bornes valident les passeports électroniques et aident à contrôler l'identité des titulaires de passeport électronique (dont les Canadiens) par la technologie de la reconnaissance faciale (vérification individuelle).
127. En 2019, les BIP ont traité 21 853 422 personnes, soit une moyenne de 59 872 voyageurs par jour¹⁸⁵. C'est dire que la plupart des gens – Canadiens ou étrangers – qui arrivent au Canada par avion voient leurs données biométriques subir une analyse quelconque (à titre d'étrangers ayant des données biométriques inscrites et/ou de titulaires de passeport électronique)¹⁸⁶. L'ASFC est habilité par l'article 11 de la *Loi sur les douanes* et les articles 15 et 18(1) de la LIPR à recueillir des renseignements auprès des gens à leur arrivée au Canada.

¹⁸³ Il s'agit des aéroports Pearson de Toronto, Trudeau de Montréal, d'Ottawa, de Vancouver, de Québec, de Winnipeg, de Calgary, d'Edmonton, de Halifax et Billy-Bishop de Toronto.

¹⁸⁴ Les BIP de première génération (1,0), mises en place en 2015, n'avaient aucune capacité VSED. Les bornes de seconde génération (2,0), mises en place de 2017 à 2019 dans le cadre du Projet d'expansion de la biométrie, ont introduit cette capacité, mais sans qu'elle soit présente dans tous les grands aéroports internationaux du pays.

¹⁸⁵ ASFC, « Primary Inspection Kiosk (PIK) Program, ePassport Validation 2020, Version 1.0 », ASFC, 9 juin 2020, p. 6 [OSSNR_202002_03_015, p. 6].

¹⁸⁶ Toutefois, les voyageurs peuvent toujours opter pour le traitement manuel s'ils le désirent. Selon l'EFVP sur les BIP, [traduction] « l'ASFC vise à faire passer 100 % des voyageurs par les BIP, [mais] un sous-groupe pourrait, par choix ou aiguillage, passer par le traitement en personne pour diverses raisons : langue, aversion pour la technologie, questions de documentation, âge, etc. ». ASFC, « Primary Inspection Kiosk (PIK) Implementation 1.0: Privacy Impact Assessment (PIA) », décembre 2016 [OSSNR_202002_03_014, p. 15]. En 2019-2020, 93,2 % des voyageurs ont employé les BIP des

128. La BIP facilite l'évaluation des risques par la transmission des informations sur le passeport et des renseignements biographiques à l'ASFC pour traitement en temps réel. L'Agence utilise cette information pour contrôler le voyageur dans les systèmes en place de traitement des voyageurs. Cela comprend le Système d'interdiction et d'alerte à la frontière et le Système intégré d'exécution des douanes¹⁸⁷.
129. Selon l'ASFC, toute l'information circule entre les BIP et l'ASFC dans un tunnel crypté et est purgée avant utilisation de la borne par le voyageur qui suit¹⁸⁸.
130. L'emploi de la photo faciale intégrée à la puce du passeport électronique permet de vérifier l'identité à la borne en cours d'inspection primaire. La reconnaissance faciale – ou « correspondance faciale » comme l'appelle l'ASFC dans ce contexte – se fait au moyen d'une vérification individuelle et, à cette fin, on extrait la photo numérique de la puce et la compare à la photo du voyageur captée en direct par la borne. Un résultat de comparaison est produit par l'algorithme exclusif du fournisseur et l'ASFC peut voir si le résultat est supérieur ou inférieur à un seuil préétabli. Le résultat est imprimé sur le reçu de la BIP¹⁸⁹. C'est l'Agence qui définit elle-même la norme de correspondance; elle n'est pas fixée par le fournisseur ni par l'administration aéroportuaire et elle ne leur est pas communiquée non plus.
131. Le reçu comporte la photo faciale saisie par la borne. Le voyageur présente le document à un agent des services frontaliers (ASF). En cas de non-correspondance, l'ASF peut corriger des erreurs non techniques évidentes (si, par exemple, quelqu'un a été photographié deux fois dans un groupe de deux) dans une vérification à vue, poser d'autres questions ou renvoyer l'intéressé à l'inspection secondaire à sa discrétion.
132. L'inclusion de la photo sur le reçu a représenté une question importante dans l'EFVP de 2012 sur le projet des BIP. L'ASFC a justifié cette pratique en parlant d'efficacité (traitement plus rapide par l'ASF qui recueille les reçus) et de sécurité (volonté d'empêcher tout échange de reçus avant la sortie d'inspection primaire)¹⁹⁰. Le reçu de la BIP – avec la photo imprimée – est conservé par l'ASFC pendant sept ans¹⁹¹. Le CPVP s'est dit préoccupé de la durée de la

aéroports là où il y en avait et l'Agence s'est fixé dans ce domaine un objectif de 95 % pour 2022. Voir ASFC, « Plan ministériel pour l'exercice 2021 à 2022 – Agence des services frontaliers du Canada », 2021. Consultation le 20 août 2021. https://www.google.com/search?q=plan+ministeriel+2021+2022+ASFC&rlz=1c1gcea_enCA801CA801&oq=plan+ministeriel+2021+2022+asfc&aqs=chrome. Disons enfin que, si le passeport électronique est désormais la règle dans le monde, il reste des passeports analogiques en circulation qui peuvent être lus par les BIP, mais sans permettre la reconnaissance faciale; les titulaires d'un passeport analogique voient l'image de leur passeport soumise à une vérification manuelle par les ASF.

¹⁸⁷ Les recherches dans ces systèmes fournissent des renseignements supplémentaires tirés de diverses sources : cibles, avis de surveillance, dossiers de mesures d'exécution antérieures, ensemble de données de l'ASFC sur les documents de voyage perdus et volés, base de données SLTD (documents de voyage et d'identité) d'INTERPOL, avis de recherche et mandats du Centre d'information de la police canadienne (CIPC). Réponse écrite de l'ASFC à l'OSSNR, 10 juin 2021, p. 2.

¹⁸⁸ Réponse écrite de l'ASFC à l'OSSNR, 6 juillet 2021, p. 2.

¹⁸⁹ Le résultat est inscrit sous forme de code sur le reçu et n'est pas interprétable par le voyageur.

¹⁹⁰ ASFC, « Primary Inspection Kiosk (PIK) Implementation 1.0: Privacy Impact Assessment », Service de traitement des voyageurs, sans date [OSSNR_202002_03_014].

¹⁹¹ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 5 - Travellers Branch (PIK & SFV) », p. 1.

conservation parce que la photo du voyageur est présente¹⁹². Pour l'essentiel, la conservation de ces photos permet de disposer d'une base de données sur la (presque) totalité des voyageurs qui entrent au pays. L'ASFC a affirmé que les photos ne sont pas consultables ni utilisées à des fins de reconnaissance faciale, mais le CPVP a jugé délicat de conserver les données biométriques¹⁹³ dans des bases d'information centralisées et a prié instamment l'Agence d'envisager des stratégies d'atténuation¹⁹⁴.

133. L'ASFC établit les spécifications et les exigences nécessaires pour les bornes d'inspection primaire, mais compte sur les administrations aéroportuaires pour fournir le matériel et les logiciels (avec l'algorithme de correspondance faciale). Il existe donc des versions différentes des BIP dans les divers aéroports au Canada. La précision du processus de correspondance faciale varie en conséquence. Les algorithmes appartiennent aux fournisseurs et l'ASFC n'a pas d'idée précise de leur fonctionnement, bien qu'ayant accès aux données sur la précision et le rendement par l'entremise du National Institute of Standards and Technology (NIST) du département du Commerce des États-Unis, et de données de tests internes de rendement.
134. En 2020, l'ASFC a évalué le rendement des quatre algorithmes de correspondance faciale intégrés aux trois conceptions de bornes en usage et a déterminé qu'il était possible d'améliorer le rendement dans certains aéroports en ajustant les seuils de correspondance¹⁹⁵. Dans les tests, on s'est de même intéressé au biais démographique possible¹⁹⁶. Les résultats témoignent de légers écarts¹⁹⁷ selon le sexe (taux de correspondance inférieurs des femmes) et l'âge (taux de correspondance inférieurs des plus jeunes et des plus âgés) dans les aéroports utilisant un algorithme particulier. Entre autres mesures d'atténuation recommandées, on envisageait des changements de fournisseurs et/ou l'établissement de seuils de correspondance spécifiques aux hommes et aux femmes, mais cette dernière possibilité était considérée comme étant susceptible d'entraîner une hausse du nombre de faux positifs.
135. Dans des rapports destinés au public, on a dit s'inquiéter de ce que des taux supérieurs d'erreurs de correspondance faciale pour certains groupes ethniques se soldent par des renvois plus fréquents au secondaire par les BIP¹⁹⁸. On a fait observer, par exemple, que les taux de renvoi au secondaire d'étrangers sont plus élevés pour l'Iran et la Jamaïque que pour l'Islande et

¹⁹² Lettre du CPVP à l'ASFC, « Re : Privacy Impact Assessment – Primary Inspection Kiosk (PIK) Implementation 1.0 », 16 octobre 2017 [OSSNR_202002_03_013, p. 4].

¹⁹³ Même si elle n'est ni utilisée ni consultable à présent à des fins de reconnaissance faciale, l'information *pourrait* servir un jour à l'analyse biométrique si on considère la qualité des photographies et l'existence de cette base de données.

¹⁹⁴ Il pourrait s'agir, par exemple, de caviarder les photographies avant de stocker le reçu ou carrément de l'éliminer, ou encore d'exiger de l'ASF qu'il examine plutôt la photographie de passeport du voyageur.

¹⁹⁵ ASFC, « Memorandum: PIK/Nexus Kiosk Performance as Function of Matching Threshold: Opportunity for Improvement in Toronto », Scientifique principal des données, 20 octobre 2020, p. 1 [OSSNR_202002_03_001, p. 1].

¹⁹⁶ ASFC, « Memorandum: Gender 'Bias' in PIK/Nexus Kiosks », Scientifique principal des données, 21 octobre 2020 [OSSNR_202002_03_002].

¹⁹⁷ Les écarts étaient de 2 à 4 %. ASFC « Memorandum: Gender 'Bias'... », p. 2 [OSSNR_202002_03_002, p. 2].

¹⁹⁸ Voir, par exemple, Evan Dyer, « Bias at the border? CBSA study finds travellers from some countries face more delays », CBC News, 24 avril 2019. Consultation le 6 août 2021. <https://www.cbc.ca/news/politics/cbsa-screening-discrimination-passports-1.5104385>; Beaumont, « When Border Security Crosses a Line »; Israël, « Facial Recognition at a Crossroads ».

le Danemark¹⁹⁹. L'ASFC a indiqué à l'OSSNR qu'aucun renvoi au secondaire ne se faisait après correspondance faciale (il n'y a pas dans ce cas de code de renvoi au secondaire par la borne d'inspection primaire). Dans la pratique cependant, une non-correspondance incitera l'ASF à examiner plus avant la cause de cette situation lors de l'inspection primaire. Il est possible qu'un renvoi discrétionnaire en résulte; l'ASFC ne suit pas les statistiques liées à un tel scénario²⁰⁰.

136. L'ASFC est consciente qu'on peut craindre un biais associé à des taux supérieurs d'erreur de correspondance faciale pour certaines catégories d'origine ethnique²⁰¹ et signale des améliorations de la précision générale des algorithmes qui aideront à combler les écarts de rendement entre les catégories démographiques. Il fait aussi observer que son [traduction] « travail dans ce domaine commence à peine sans rien de concluant et avec encore beaucoup de travail à faire ». Vu le grand intérêt et la sérieuse crainte du public quant à la possibilité d'un biais, l'OSSNR encourage l'ASFC à poursuivre son travail en la matière. Outre les solutions techniques qui visent à combler les lacunes constatées, des mesures d'atténuation stratégiques pourraient être établies à la suite de l'examen des conséquences des erreurs de correspondance faciale sur les voyageurs.

137. Les BIP continueront à jouer un rôle essentiel pour les futures applications de la technologie biométrique dans les aéroports internationaux du Canada. Comme le mentionne le Plan ministériel pour l'exercice 2021-2022 de l'ASFC, l'organisme est prêt à intégrer les BIP aux nouvelles applications de technologie mobile dans le but de simplifier davantage le traitement des arrivées à la douane et à l'immigration.

¹⁹⁹ Dyer, « Bias at the border? » L'ASFC a réagi à ces observations en disant qu'une [traduction] « analyse au niveau macro [...] n'avait relevé aucun indice systématique de distinction illicite » et que les différences de taux de renvoi tenaient probablement à des différences moyennes entre populations quant aux motifs de demande d'entrée au Canada (plus d'Iraniens visaient à s'établir, d'où un appel à la vigilance, et plus d'Islandais venaient faire du tourisme).

²⁰⁰ En revanche, l'ASFC suit bel et bien les renvois à l'inspection secondaire après vérification des empreintes digitales. À l'exercice 2020-2021, on a dénombré au total 300 033 renvois à l'inspection secondaire par les BIP. Sur ce nombre, 28 998 relevaient du code « Vérification biographique requise », ce qui indiquait que la vérification dans les bases de données de la GRC s'était révélée incomplète et non concluante et avait donné un résultat de non-correspondance. Réponse écrite de l'ASFC à l'OSSNR, 10 juin 2021, p. 4 et 5.

²⁰¹ ASFC, « Biometrics (Face Recognition) in ASFC: Overview of Latest Research Findings, Networks and Resources », bureau de la dirigeante principale des données, 1^{er} octobre 2020 [OSSNR_202002_03_003].

NEXUS

138. NEXUS est un programme pour les dignes de confiance, auquel la participation est volontaire, qui vise à accélérer le passage à la frontière canado-américaine dans le cas des voyageurs à faible risque déjà approuvés (« NEXUS »)²⁰². Le paragraphe 11.1(1) de la *Loi sur les douanes* habilite le ministre à administrer de tels programmes en lui permettant d'accorder à quiconque une autorisation de se présenter à la frontière selon « un mode substitutif »²⁰³. Le programme NEXUS est cogéré par l'Agence et la US Customs and Border Protection (CBP)²⁰⁴. Comme il est mentionné à la section IV, si NEXUS a vu le jour comme initiative pilote avant les attentats du 11 septembre, il a été élargi et mis en œuvre après les attentats avec à l'esprit de solides mesures de vérification de l'identité et de facilitation des mouvements des voyageurs dans un contexte de renforcement de la sécurité frontalière.
139. En 2019, NEXUS a été soumis à un processus de « modernisation », notamment l'intégration du modèle de correspondance faciale des BIP aux bornes réservées à NEXUS pour les arrivées par avion²⁰⁵, ce qui remplaçait la lecture de l'iris par la correspondance faciale comme modalité biométrique de vérification de l'identité²⁰⁶. Pour faciliter cette correspondance, l'ASFC recueille les données biométriques des passeports électroniques, les verse dans la base de données NEXUS et se sert de la photo pour vérifier l'identité pendant le voyage²⁰⁷. Ce processus est semblable à la manière de fonctionner des BIP pour d'autres catégories de voyageurs et produit des résultats à peu près semblables²⁰⁸. La grande différence est que la photo prise à la borne est comparée à l'image du voyageur dans la base de données NEXUS²⁰⁹. Le but avec l'utilisation de la photo de passeport dans NEXUS est le même que pour le traitement ordinaire aux BIP qui consiste à vérifier l'identité du voyageur avant de le laisser entrer au pays. L'emploi de la photo de passeport dans NEXUS a été jugé préférable, parce que l'image assure une meilleure comparaison de reconnaissance faciale (ayant été prise suivant les spécifications de l'OACI) si on

²⁰² Les demandeurs font l'objet d'un contrôle préalable dans les bases de données de la criminalité, de l'immigration et des douanes.

²⁰³ Il s'agit d'une solution de rechange au paragraphe 11(1) de la *Loi sur les douanes* qui exige que quiconque arrive au Canada passe nécessairement à un bureau de douane, doté des attributions prévues à cet effet, qu'il se présente sans délai à un agent et qu'il réponde véridiquement aux questions qui lui sont posées. Voir aussi le *Règlement de 2003 sur l'obligation de se présenter à un bureau de douane*, article 6.1, et le RIPR, paragraphe 38a).

²⁰⁴ La composition est environ d'20 % d'Américains et 80 % de Canadiens. ASFC, « NEXUS Modernization Air Mode », 7 juin 2018, p. 4 [OSSNR_202002_004, p. 4].

²⁰⁵ Cette section porte principalement sur NEXUS dans le mode aérien (NEXUS aux points d'entrée aériens); le programme NEXUS offre dans la même optique un traitement accéléré aux points d'entrée terrestres (21 grands points terrestres au Canada) et aux points d'entrée maritimes (22 points NEXUS seulement). Notons toutefois qu'aucune analyse biométrique à caractère technologique n'a lieu dans les modes terrestres et maritimes NEXUS. Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 4 – Travellers Branch (NEXUS program) », p. 1.

²⁰⁶ ASFC, « NEXUS Modernization Air Mode », 7 juin 2018 [OSSNR_202002_004].

²⁰⁷ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 4 – Travellers Branch (NEXUS program) », p. 2.

²⁰⁸ ASFC, « PIK/NEXUS Kiosks: Performance Audit Report », 21 mai 2020 [OSSNR_202002_03_005].

²⁰⁹ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 4 – Travellers Branch (NEXUS program) », p. 3.

la compare à la photo de l'adhésion à NEXUS (prise par les agents des services frontaliers dans diverses conditions de lumière, d'arrière-plan, de distance, etc.)²¹⁰. Les participants à NEXUS sont informés de l'extraction de la photo de leur passeport à des fins de mise en correspondance faciale.

140. La nature volontaire de la participation à NEXUS et la cohérence de la volonté d'y employer la photo de passeport pour faciliter la vérification d'identité et les mouvements rendent raisonnable cet autre usage de la photo de passeport électronique aux yeux de l'OSSNR. La compatibilité des objectifs de ces programmes respecte aussi les normes et les exigences des articles 7 et 8 de la *Loi sur la protection des renseignements personnels*.
141. L'utilisation de la photo de passeport à des fins de mise en correspondance faciale dans le programme NEXUS est néanmoins digne de mention comme exemple de cas où il a été avantageux d'utiliser une biométrie existante dans un nouveau programme. Le double usage ici de la biométrie est relativement anodin, mais la dynamique de sa production c'est-à-dire la commodité, la disponibilité et l'éventuelle valeur ajoutée (fidélité de l'identification) de l'information biométrique existante pourrait se retrouver dans des scénarios peut-être plus préoccupants comme nous le verrons (voir les paragraphes 191 à 201 plus loin).

6. AVENIR DE LA BIOMÉTRIE

142. Nous nous attendons à ce que le panorama que nous avons décrit en détail dans les sections qui précèdent évolue nettement à court, à moyen et à long terme. Dans la présente section, nous mettrons certains projets ou initiatives en évidence pour illustrer comment la biométrie pourrait évoluer dans le continuum frontalier et pour souligner les grands points à considérer pour les Canadiens et l'OSSNR à mesure que nous nous dirigeons vers cet avenir technologique qui s'offre à nous.
143. Le gouvernement du Canada s'est engagé publiquement à poursuivre les mesures de recherche-développement et de déploiement pour les technologies biométriques du continuum frontalier. Ainsi, le budget de 2021 affecte 656,1 M\$ sur cinq ans (à compter de 2021-2022) et 123,8 M\$ par la suite à l'ASFC pour la « modernisation » des frontières canadiennes²¹¹. L'ASFC « propose le recours à de nouvelles technologies, comme la reconnaissance faciale et la vérification des empreintes digitales²¹² » dans le cadre de cette modernisation.

²¹¹ Gouvernement du Canada, « Budget 2021 : Une relance axée sur les emplois, la croissance et la résilience », 2021. Consultation le 8 août 2021. <https://www.budget.gc.ca/2021/home-accueil-fr.html>, p. 163.

²¹² Gouvernement du Canada, « Budget 2021 », p. 587.

144. L'Agence a annoncé la création d'un Bureau de la biométrie et de la gestion de l'identité (BBGI)²¹³ relevant de la nouvelle Direction de la transformation de la biométrie (DTB) au sein de la Direction générale du dirigeant principal de la transformation (DGDPT). Elle a indiqué à l'OSSNR que le mandat de la DTB est de coordonner les initiatives (conception, mise en œuvre et fonctionnement) liées à la biométrie à l'échelle de l'organisme. En dehors de son rôle de coordination, le Bureau de la biométrie et de la gestion de l'identité sera le centre d'expertise et de liaison au sein de l'Agence en ce qui a trait au bon usage de la biométrie. Il s'agira notamment de concevoir et de gérer un cadre de gouvernance, de gestion des risques et de vérification de la conformité pour la biométrie à l'ASFC²¹⁴. En juin 2021, on a sollicité dans un Avis de projet de marché (APM) des propositions d'entrepreneurs pour aider à établir ce bureau et « travailler avec [l'Agence] pour rechercher, planifier et développer rapidement une stratégie et une feuille de route liées à l'utilisation de solutions numériques rendues possibles grâce aux technologies de soutien en biométrie, en réponse à la situation de la COVID-19 et à d'autres priorités opérationnelles²¹⁵ ». L'appel de propositions disait également de l'entrepreneur retenu qu'il « aidera l'ASFC à élaborer une approche et un plan complets pour gérer, évoluer et s'adapter à l'utilisation de la biométrie²¹⁶ » aux fins de la réalisation du mandat et des objectifs de l'Agence. Dans cette fonction de coordination, le Bureau de la biométrie et de la gestion de l'identité passera en revue les activités biométriques établies et fera les recommandations nécessaires pour les harmoniser avec les normes et les objectifs globaux de l'ASFC²¹⁷.
145. En matière d'immigration, l'ASFC s'engage dans son Plan ministériel pour l'exercice 2021-2022 à « étudier des mesures visant à normaliser la collecte de renseignements biométriques sur les voyageurs potentiellement interdits de territoire afin de renforcer la vérification de la conformité à la frontière²¹⁸ ». En juillet 2021, IRCC a publié un avis d'appel d'offres où il sollicitait des renseignements de l'industrie au sujet de l'acquisition d'un Système canadien d'identification biométrique aux fins d'immigration (SCIBI) de nouvelle génération²¹⁹. Le nouveau système [traduction] « tirera parti des plus récentes technologies [...] pour moderniser la solution

²¹³ La Presse canadienne, « Canada's border agency urgently developing biometric plans in response to COVID-19 », CTV News, 7 juin 2021. Consultation le 8 août 2021. <https://www.ctvnews.ca/health/coronavirus/canada-s-border-agency-urgently-developing-biometric-plans-in-response-to-covid-19-1.5459521>.

²¹⁴ Réponse écrite d'IRCC à l'OSSNR, 1^{er} octobre 2021.

²¹⁵ Services publics et Approvisionnement Canada, « Biométrie et gestion des identités (1 000 357 607) », 14 juin 2021. Consultation le 8 août 2021. <https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-21-00958775>.

²¹⁶ Services publics et Approvisionnement Canada, « Biométrie et gestion des identités (1 000 357 607) ».

²¹⁷ Réponse écrite de l'ASFC à l'OSSNR, 22 juillet 2021, p. 1.

²¹⁸ ASFC, « Plan ministériel pour l'exercice 2021-2022 », p. 20.

²¹⁹ Services publics et Approvisionnement Canada, « SCIBI Génération Prochaine LD (B8465-220030/A) », 29 juillet 2021. Consultation le 10 août 2021. <https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-XQ-012-39765>.

technologique en biométrie [d'IRCC] » et pourrait comporter [traduction] « la conception et la mise au point d'une nouvelle solution sur mesure de collecte de données biométriques pour IRCC »²²⁰.

146. On assiste également à la naissance d'une version de « prochaine génération » du Programme de passeport, laquelle prendra la forme d'« un nouveau livret de passeport intégrant les avancées technologiques pour améliorer la durabilité et les caractéristiques de sécurité du document²²¹ ». Le but est en partie d'améliorer la « concordance avec les documents de nos partenaires du Groupe de passeport des Cinq nations²²² ». La mise en place progressive du nouveau passeport électronique aura lieu en 2023 et 2024.
147. La délivrance des passeports connaît dans la même optique une « modernisation » dans le cadre d'une démarche en cours depuis 2013 qui vise à faciliter le passage du Programme de passeport du ministère des Affaires étrangères, du Commerce et du Développement à CIC (aujourd'hui IRCC). L'Initiative de modernisation du Programme de passeport (IMPP) est un projet pluriannuel qui devrait se terminer en 2023. L'IMPP vise à rationaliser « tous les aspects des activités du Programme de passeport » et à « rester au fait des meilleures pratiques internationales en matière de gestion de l'identité et de délivrance de permis »²²³. Il s'agit aussi d'« accroître l'accès des Canadiens aux services de passeport en leur offrant la plateforme nécessaire à la prestation de services en personne uniformes dans un plus grand nombre d'endroits au Canada, et en jetant les bases des services de passeport en ligne et de l'automatisation pour améliorer l'expérience de service »²²⁴.
148. En juin 2020, IRCC a produit un Avis de projet de marché (APM) pour un « projet de services numériques de passeport » qui « permettra aux Canadiens de présenter une demande de passeport en ligne au moyen d'un ordinateur, d'une tablette ou d'un appareil mobile comme solution de rechange pratique aux options de service par la poste ou en personne²²⁵ ». La plateforme visée par ce projet d'acquisition transmettra les demandes de passeport – avec les photos numériques – des particuliers à IRCC. Au début de 2021, les médias ont annoncé qu'IBM avait été le soumissionnaire retenu²²⁶. Le système projeté a suscité des inquiétudes en matière de protection des renseignements personnels, surtout en ce qui concerne la transmission de

²²⁰ Services publics et Approvisionnement Canada, « SCIBI Génération Prochaine LD (B8465-220030/A) », 29 juillet 2021. Consultation le 10 août 2021. <https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-XQ-012-39765>, p. 2.

²²¹ IRCC, « Évaluation du Programme de passeport », p. 35.

²²² IRCC, « Rapport d'étape sur les projets de transformation et les grands projets de l'État », 10 mars 2020. Consultation le 11 août 2021. <https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/publications-guides/plan-ministeriel-2020-2021/rapport-etape-sur-projets-transformation-grands-projets-etat.html>.

²²³ IRCC, « Rapport d'étape sur les projets de transformation et les grands projets de l'État ».

²²⁴ IRCC, « Rapport d'étape sur les projets de transformation et les grands projets de l'État ».

²²⁵ Services publics et Approvisionnement Canada, « Projet des services numériques de passeport », 22 juin 2020. Consultation le 11 août 2021. <https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-XS-002-38054>.

²²⁶ Estelle Côté-Sroka, « Virtual passport app presents real data risk, experts warn », CBC News, 22 février 2021. Consultation le 11 août 2021. <https://www.cbc.ca/news/canada/ottawa/passport-application-online-program-1.5920625>.

renseignements biométriques (et de photos numériques) par le biais d'une plateforme privée²²⁷. On peut s'attendre à ce que la tension évoquée entre commodité et confidentialité devienne ces prochaines années une ligne de force du débat public sur les nouvelles activités biométriques.

149. Dans le même ordre d'idées, le Plan ministériel pour l'exercice 2021-2022 de l'ASFC met en évidence un certain nombre d'initiatives d'expérimentation et d'innovation en technologie mobile (téléphones intelligents, par exemple), « pour explorer les concepts d'identité numérique et les possibilités de les mettre à l'essai dans le continuum des voyages du point de vue de la gestion de la frontière ». Cette notion d'identité numérique vise une identification sans papier où la preuve numérique fiabilisée et sécurisée de l'identité d'une personne remplace les documents qui autrefois étaient en format papier (passeports, permis de conduire, etc.)²²⁸.
150. La biométrie permet normalement de lier une identité numérique à une personne. La première version (type 1) du document de voyage numérique (DVN) de l'OACI, par exemple, fait le lien entre le voyageur et son identité numérique par des données biométriques intégrées au passeport électronique; il est ainsi moins fréquent de devoir produire le document papier lors de déplacements²²⁹. Les documents de voyage numériques relèvent d'un projet international qui, sous la coordination de l'OACI, tient compte des commentaires de tous les pays du monde et prévoit plusieurs futures versions de ces documents (types 2 et 3). IRCC et l'ASFC font actuellement partie du Groupe de travail des nouvelles technologies (GTNT) et de son sous-groupe des DVN. La vision à long terme qui anime ce projet est celle du remplacement des passeports sur papier par des « jetons d'identité numérique » (comprenant la photo faciale du passeport) stockés sur appareil mobile²³⁰.
151. Comme il a été indiqué à la section IV, le projet FASTER-PrivBio (2015-2017) d'IRCC et de l'ASFC a aussi exploré l'utilisation de jetons d'identité stockés dans une application mobile dans

²²⁷ Côté-Sroka, « Virtual passport app presents real data risk ». Dans une réponse écrite à l'OSSNR le 1^{er} octobre 2021, IRCC a fait observer ce qui suit : [traduction] « IBM est le soumissionnaire retenu, mais la solution a été déployée dans le nuage Protégé B d'IRCC. Cette solution est conforme aux lignes directrices du SCT. Tous les renseignements personnels des Canadiens sont sous le contrôle d'IRCC. De plus, le Ministère a soumis à une EFVP la nouvelle [...] solution dans le cadre de cette initiative pilote en vue de permettre de reconnaître et de trouver le moyen de régler toute autre préoccupation en matière de vie privée. Le CPVP a participé au processus d'élaboration de cette initiative. »

²²⁸ La mise en œuvre des « identités numériques » devrait prendre de l'ampleur ces prochaines années dans les secteurs et privé et public. Un organisme comme le Conseil d'identification et d'authentification numériques du Canada (CIAN), (<https://diacc.ca/the-diacc/>), qui est une coalition sans but lucratif d'entités du secteur privé et du secteur public, propose de mettre en place un « écosystème numérique » où une identité numérique commune et reconnue serait transférable entre les contextes (depuis la demande de prêt hypothécaire jusqu'à l'accès aux services gouvernementaux). Voir aussi Identity North (<https://www.identitynorth.ca/>).

²²⁹ R. Rajeshkumar, « Digital Travel Credentials », OACI, mai 2021. Consultation le 10 août 2021. <https://www.icao.int/Meetings/TRIP-Symposium-2021/PublishingImages/Pages/Presentations/Digital%20Travel%20Credential%20%28DTC%29%20Policy%20and%20Guiding%20Principles.pdf>.

²³⁰ OACI, « The ICAO Digital Travel Credential », mars 2020 [OSSNR_202002_012].

le contexte des autorisations de voyage électroniques (AVE). Ce projet a pris fin en 2017 et sa « phase II » est devenue l'initiative Chaîne de confiance (CdC) que dirige l'ASFC avec la collaboration d'IRCC, de Recherche et développement pour la défense Canada (RDDC), de l'Université d'Ottawa et de partenaires de l'industrie.

152. Dans le projet « Chaîne de confiance », on a considéré l'adoption de la technologie mobile dans le processus AVE en incluant également d'autres étapes du continuum des voyages. Voici ce que décrit l'ASFC dans son Rapport sur Objectif 2020 » (publié en décembre 2018) :

« Pour profiter de la chaîne de confiance, les voyageurs devraient télécharger une application sur leur téléphone intelligent et se créer un compte incluant un identificateur unique basé sur leurs données biométriques. À toutes les étapes du voyage, de la réservation des vols au débarquement de l'avion, en passant par l'obtention de la carte d'embarquement, les données du voyageur seraient captées pour accélérer son passage. Avant l'atterrissage, le voyageur devrait produire une déclaration électronique et la signer de façon numérique au moyen de la vérification faciale biométrique du visage. À l'arrivée du voyageur, des caméras de vérification faciale associeraient le voyageur à son identificateur unique²³¹. »

153. Le but ultime du processus est d'améliorer l'évaluation des risques. Lier l'information sur les voyageurs à leur identité dans tout le continuum des voyages (ce qui comprend le recours à la reconnaissance faciale lorsque le voyageur circule dans l'aéroport) vient faciliter les mouvements des voyageurs à faible risque (cela permet notamment de réduire au minimum les points de contact avec le contrôle frontalier, caractéristique qui gagnera en importance dans le contexte des voyages après la pandémie de COVID-19), tout en améliorant la détection des voyageurs à haut risque.

154. En 2018, un prototype en simulation a démontré les caractéristiques et le déroulement du processus de la Chaîne de confiance aux représentants du gouvernement canadien²³². Le projet impliquant le prototype a pris fin en 2019, mais l'initiative générale Chaîne de confiance se poursuit selon le Plan ministériel pour l'exercice 2021-2022 de l'ASFC par la mise en place de « produits minimaux viables à petite échelle pour évaluer la faisabilité dans un environnement réel et obtenir des commentaires sur l'expérience des utilisateurs²³³ ». Le but déclaré avec la Chaîne de confiance demeure « de simplifier l'identification des voyageurs grâce à l'utilisation de titres de voyage numériques et de la biométrie²³⁴ ». Fait digne de mention, la CdC s'harmonise directement avec d'autres initiatives et projets internationaux comme le projet des documents de

²³¹ ASFC, « ASFC – Rapport sur Objectif 2020 : Prototype de la chaîne de confiance », décembre 2018. Consultation le 10 août 2021. <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/bp2020/2018/trust-confiance-fra.html>.

²³² World Reach, « Canada's Chain of Trust Project – Seamless Travel », sans date. Consultation le 10 août 2021. <https://worldreach.com/resources/video-library/canadas-chain-of-trust-seamless-travel/>.

²³³ ASFC, « Plan ministériel pour l'exercice 2021-2022 », p. 19.

²³⁴ ASFC, « Plan ministériel pour l'exercice 2021-2022 », p. 19.

voyage numériques (DVN) de l'OACI²³⁵, ce qui témoigne du degré de coordination qui existe dans l'écosystème plus global de l'expérimentation biométrique.

155. Soyons clairs : les caractéristiques de la Chaîne de confiance que nous avons décrites ne sont pas le reflet de ce qui se fait actuellement à la frontière et ne représentent pas non plus un engagement de l'ASFC (ou de toute autre entité du gouvernement du Canada) en matière d'expérience future des voyageurs. Au moment où sera réalisée cette chaîne, une certaine version de ce qu'elle doit être ou un nouveau projet de la même veine, la façon précise dont la biométrie vérifie l'identité ou dont les voyageurs se déplacent à travers l'aéroport pourrait avoir nettement changé. Les grandes tendances sont néanmoins apparentes, puisque l'identité numérique, la technologie mobile et la vérification biométrique sont de plus en plus appelées à orienter l'expérience du voyageur.
156. Un autre exemple est le projet pilote « identité numérique des voyageurs connus » que dirige Transports Canada en collaboration avec le Forum économique mondial (FEM), le gouvernement des Pays-Bas et des partenaires commerciaux. En 2018, le Canada a annoncé qu'il adhère activement à la vision plus large d'INVC du FEM²³⁶ et, en 2019, à un projet pilote de validation de principe entre des aéroports canadiens (Pearson à Toronto et Trudeau à Montréal) et néerlandais (Schiphol à Amsterdam) pour les vols d'Air Canada et de KLM Royal Dutch Airlines²³⁷. Ce projet pourrait obtenir les fonds nécessaires dans le budget de 2021 qui propose 105,3 M\$ sur cinq ans pour la conception d'une approche en matière d'identité numérique à l'intention des voyageurs aériens²³⁸.
157. L'initiative INVC joindra la technologie de la chaîne de blocs²³⁹ à celle de la reconnaissance faciale [traduction] « afin de faciliter par une application mobile une expérience harmonieuse et

²³⁵ Parmi ces autres initiatives ou projets, on compte le « Safe and Seamless Traveller Journey » du World Travel & Tourism Council et le « OneID » de l'IATA. World Reach, « Chain of Trust – Canada », 2020. Consultation le 10 août 2021.

https://worldreach.com/wp-content/uploads/2019/11/CaseStudy_CanadaChainofTrustProject_v2.pdf.

²³⁶ Transports Canada, « Le gouvernement du Canada mettra à l'essai des technologies de pointe favorisant la sûreté et la fluidité des déplacements des voyageurs aériens dans le monde entier », communiqué de presse, 25 janvier 2018.

Consultation sur le 10 août 2021. https://www.canada.ca/fr/transports-canada/nouvelles/2018/01/le_gouvernement_ducanadamettraalessaidestechnologiesdepointefavo.html.

²³⁷ Toronto Pearson, « Toronto Pearson s'associe au gouvernement et à l'industrie pour un projet pilote de voyages sans papier », communiqué de presse. 26 juin 2019. Consultation le 10 août 2021.

<https://www.torontopearson.com/fr/entreprise/medias/communiqués-de-presse/2019-06-26>.

²³⁸ Gouvernement du Canada, « Budget de 2021 », p. 83.

²³⁹ Les chaînes de blocs sont des registres numériques inviolables et inaltérables qui sont mis en œuvre en mode réparti (sans dépôt central) et normalement aussi sans autorité centrale (banque, société ou gouvernement). À la base, elles permettent à une communauté d'utilisateurs d'enregistrer des opérations dans un registre que partage la collectivité, de sorte que, en cas de fonctionnement normal de la chaîne de blocs, aucune transaction ne puisse être modifiée une fois publiée. NIST, « Blockchain Technology Overview », 8 octobre 2018. Consultation le 15 septembre 2021.

<https://www.nist.gov/publications/blockchain-technology-overview>.

sécuritaire du transport aérien²⁴⁰ ». Les voyageurs verront leur photo faciale captée pour une vérification individuelle avec leur photo de passeport électronique à différents points de contact du continuum des voyages (embarquement, passage à la douane, etc.). Ils pourront transmettre leur information (dont leurs données biométriques faciales) au partenaire concerné (sociétés aériennes ou douanes néerlandaises ou canadiennes) s'ils le souhaitent ou revenir en tout temps à la vérification classique de l'identité (sur passeport électronique, par exemple). Transports Canada contrôlera, au moyen d'une interface avec l'ASFC, les passeports électroniques au moment de l'inscription (pour en vérifier l'authenticité et s'assurer qu'il ne s'agit pas d'un document perdu ou volé) et aucune évaluation des risques n'aura lieu pour les passagers.

158. Au moment où nous écrivons ces lignes, le projet pilote n'est pas encore en vigueur. La pandémie de COVID-19 a influé tant sur les délais que sur le contexte opérationnel du projet. Au départ, l'initiative INVC visait en partie à traiter des volumes croissants de voyageurs, mais la pandémie a réduit ces volumes et amplifié la nécessité d'un traitement avec peu de contacts ou « sans contact²⁴¹ ». En fait, l'engagement budgétaire mentionné au paragraphe 156 était lié à l'investissement du gouvernement du Canada « pour permettre la reprise des déplacements aériens en toute sécurité [...] en prévenant la transmission de la COVID-19 et en protégeant les voyageurs²⁴² ». Aux fins du présent document, l'importance de cette initiative réside dans le fait qu'elle permet de voir la trajectoire générale de la biométrie dans le transport aérien et le continuum frontalier.
159. L'initiative pilote INVC au Canada tire son origine de la vision plus large de la question qui a été établie par le Forum économique mondial. Selon le FEM, les passeports seraient effectivement remplacés par des titres numériques stockés sur appareil mobile et des points de contrôle par reconnaissance faciale (souvent appelés barrières intelligentes ou électroniques) permettraient aux voyageurs de se déplacer dans l'aéroport – arrivée, embarquement, dédouanement, sortie – avec peu ou pas d'interruption²⁴³. D'autres éléments de l'expérience du voyageur (location de chambres d'hôtel et de voitures ou magasinage à la boutique hors taxes) seraient intégrés. Au fil du temps, les voyageurs accumuleraient une liste d'interactions – ou d'« attestations » – en provenance de diverses entités (contrôle frontalier, entités commerciales) dont la somme permettrait d'établir sa fiabilité. Des profils de risque complétés par des contrôles de sécurité aideraient à établir le degré d'attention que les autorités compétentes devraient accorder à un voyageur. Ajoutons que le « portefeuille » de l'identité numérique (application mobile en mode crypté) comprendrait plus que les renseignements du passeport et les données

²⁴⁰ Information de Transports Canada à l'OSSNR, 20 juillet 2021, diapositive 3.

²⁴¹ Voir l'analyse dans « How biometrics can help airlines take off again », *Biometric Technology Today*, 2021 (1) : 8 à 11. [https://doi.org/10.1016/S0969-4765\(21\)00010-2](https://doi.org/10.1016/S0969-4765(21)00010-2). Consultation le 5 octobre 2021.

²⁴² Gouvernement du Canada, « Budget 2021 », p. 83. Voir aussi la mention de l'initiative « INVC » dans les débats parlementaires du 20 avril 2021. Consultation le 10 août 2021. <https://www.noscommunes.ca/DocumentViewer/fr/43-2/chambre/seance-84/debats>.

²⁴³ La reconnaissance faciale à l'enregistrement, à la consigne, à la sécurité, à l'embarquement, etc., limiterait le nombre d'interactions des voyageurs avec les préposés de l'aéroport.

biométriques; on y trouverait également des renseignements bancaires, le dossier de santé (et les preuves de vaccination), les diplômes d'études, les cotes de solvabilité, etc²⁴⁴.

160. Cette vision plus large est ambitieuse. Le projet pilote INVC au Canada – même avec une évolution en fonction des priorités de l'après-COVID – est décidément plus circonspect dans ses visées. Transports Canada a dit clairement dans ses communications avec l'OSSNR que le projet pilote (bien qu'ayant le FEM comme partenaire) se distingue de la vision plus générale du FEM et n'est pas tenu de s'y conformer. Il reste que l'ambition même de cette conception révèle une tendance probable pour l'avenir des voyages internationaux. Comme notre rapport le démontre, le recours à la biométrie tend à prendre de l'ampleur avec le temps. Les progrès concomitants de la technologie mobile – avec la mise au point de plateformes d'identité numérique sécurisées reposant sur la biométrie – mènent naturellement à une application dans le continuum frontalier, où l'identification est clé et, de plus en plus aussi, la commodité²⁴⁵.
161. Toutefois, il faut toujours trouver un équilibre entre une plus grande commodité et la protection de la vie privée, plus particulièrement en ce qui concerne la technologie de reconnaissance faciale. Cela suscite un important débat public au sujet de l'autorité légale de recourir à la reconnaissance faciale dans les lieux publics. Partout dans le monde, les pays se demandent comment gérer la prolifération des technologies de reconnaissance faciale, tantôt décrétant des moratoires tantôt y allant carrément d'interdictions de nouvelles applications de cette technique tant que ses conséquences n'auront pas été dûment prises en considération et que de nouveaux cadres juridiques et/ou réglementaires ne viendront pas régir son utilisation²⁴⁶.

²⁴⁴ Forum économique mondial, « Digital Borders: Enabling a secure, seamless, and personalized journey », livre blanc, janvier 2017. Consultation le 10 août 2021.

http://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf. Voir aussi Forum économique mondial, « The Known Traveller : Unlocking the potential of digital identity for secure and seamless travel », System Initiative on Shaping the Future of Mobility, janvier 2018. Consultation le 10 août 2021.

http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

²⁴⁵ IATA, « Global Passenger Survey (2019) », consultation le 4 octobre 2021. <https://www.iata.org/en/pressroom/pr/2019-10-16-01/>

²⁴⁶ Voir l'analyse de « Restriction on the use of facial recognition technologies », dans Krisztina Huszti-Orbán et Fionnuala Ní Aoláin, « Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? » Human Rights Center : Université du Minnesota. 2020. Consultation le 12 août 2021.

<https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf>, p. 26. Voir aussi le Science and Technology Committee au Royaume-Uni, « Current and future uses of biometric data and technologies », février 2015. Consultation le 18 août 2021.

<https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/73402.htm>. À noter l'appel à décréter des moratoires de la Commission européenne et du chef de la direction d'Alphabet, Sundar Pichai, comme il est évoqué dans Taylor Owen et Nasma Ahmed, « Let's face the facts: To ensure our digital rights, we must hit pause on facial-recognition technology », *The Globe and Mail*, 14 février 2020. Consultation le 12 août 2021. <https://www.theglobeandmail.com/opinion/article-lets-face-the-facts-to-ensure-our-digital-rights-we-must-hit-pause/>. Pour un exemple dans le contexte canadien, voir la lettre de Charlie Angus, député de la circonscription de Timmins-Baie James au ministre de la Justice et procureur général du Canada, David Lametti, au sujet de l'utilisation par la GRC du logiciel Clearview-AI de reconnaissance faciale, 2 mars 2020. Consultation le 4 octobre 2021. <https://www.charlieangus.ca/post/rcmp-use-of-clearwater-ai-s-facial-recognition-software>.

Les recherches récentes du CPVP sur l'utilisation de Clearview-AI par la GRC rendent compte du versant canadien de ce débat plus vaste.

162. Le débat cherche essentiellement à déterminer si les cadres existants de traitement des renseignements personnels (qui, dans certains cas, datent de plusieurs décennies et remontent à une époque antérieure à l'avènement de la reconnaissance faciale et d'autres technologies biométriques) sont suffisants et si des mesures législatives portant expressément sur la reconnaissance faciale s'imposent²⁴⁷. Une législation plus précise permettrait d'établir des normes déterminant quand le recours à la reconnaissance faciale est approprié et raisonnable. Cela accroîtrait également la transparence des normes édictées par le Parlement et informerait la population des circonstances dans lesquelles le Parlement considère que la reconnaissance faciale est légitime et raisonnable pour promouvoir la sécurité et la commodité dans la société canadienne²⁴⁸.
163. Le CPVP est en voie d'élaborer un nouveau guide sur la protection de la vie privée sur la biométrie à l'intention des secteurs public et privé, le but étant d'orienter la façon dont la technologie sera appliquée à l'avenir. Même si le contexte frontalier est différent des autres cadres publics en ce qui a trait à la confidentialité, l'utilisation de la technologie biométrique à la frontière doit se conformer aux nouvelles normes juridiques et sociétales. La mise en place de nouvelles activités doit tenir compte de ces défis et tenir compte des changements de panorama juridique et réglementaire.
164. Les préoccupations du public seront probablement des plus vives au sujet de l'utilisation de la reconnaissance faciale à tout moment dans un lieu donné, comme pour le projet pilote FOTM dont nous avons parlé à la section IV. La vérification statique et individuelle de l'identité à des bornes mobiles – comme à l'heure actuelle avec les bornes d'inspection primaire – est bien établie et permet aux voyageurs de savoir quand il y a reconnaissance faciale. La reconnaissance faciale de personnes en mouvement et l'identification collective, où les données biométriques sont captées à distance, causent plus d'anxiété. Songeons, par exemple, à la contestation

²⁴⁷ Voir, par exemple, les analyses de divers cas de reconnaissance faciale dans INCLO, « In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World », janvier 2021. Consultation le 11 août 2021. <https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf>. Voir aussi la déclaration du Technology Policy Committee de l'Association for Computing Machinery aux États-Unis, « Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies », 30 juin 2020. Consultation le 11 août 2021. <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf>. Voir enfin l'analyse de la « légitimité » dans les Guidelines on Facial Recognition du « Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel » au Conseil de l'Europe, 28 janvier 2021. Consultation le 11 août 2021. <https://edoc.coe.int/fr/intelligence-artificielle/9753-guidelines-on-facial-recognition.html>, p. 4.

²⁴⁸ Voir, par exemple, gouvernement du Canada, « Engagement de transparence en matière de sécurité nationale », 22 décembre 2020. Consultation le 12 août 2021. <https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html>.

judiciaire de ce type de recours à la reconnaissance faciale au Royaume-Uni²⁴⁹ et les appels multiples à un moratoire sur son utilisation dans les lieux publics²⁵⁰.

165. Compte tenu des faits que nous venons de décrire, l'OSSNR s'attend à ce que les renseignements biométriques soient à l'avenir désormais systématiquement intégrés à l'expérience du voyageur dans le continuum frontalier. Les considérations de sécurité et la gestion générale de l'identité garderont leur importance, mais il en va de même de la commodité pour le voyageur et, à la suite de la COVID-19, des mouvements des voyageurs « sans contact » ou « sans congestion ». Le recours à la technologie mobile et à l'identité numérique est le reflet de tendances sociétales qui se prêtent tout particulièrement à une application dans le continuum frontalier. Le consentement éclairé et/ou une habilitation juridique expresse et transparente sont des considérations importantes si on veut s'assurer que cette application est légitime et repose sur une bonne compréhension par la population du moment où les données biométriques sont recueillies, de la façon dont elles sont utilisées et des mesures prises par le gouvernement pour protéger les données dont il dispose.

7. OBSERVATIONS

166. Dans le présent rapport, nous avons documenté et décrit le recours à la biométrie par le gouvernement du Canada dans le continuum frontalier. Les activités en question sont d'une portée vaste et croissante. Pour le gouvernement, les renseignements biométriques confèrent de fermes assises à la gestion de l'identité. Par ailleurs, des groupes de la société civile, des universitaires et d'autres Canadiens concernés se préoccupent des conséquences sur la vie privée quand le gouvernement se met à recueillir, à utiliser, à conserver et à communiquer des renseignements sur des caractéristiques physiques immuables. La présente étude visait foncièrement à éclairer le débat en cours en tâchant à la fois de démystifier les activités qu'exerce actuellement le gouvernement et de les évaluer du point de vue unique et transversal qu'est celui de l'OSSNR. Dans cette dernière section, nous nous appuyons sur ce point de vue pour formuler nos observations sur neuf thèmes généraux.

1. Biométrie et sécurité nationale

167. La biométrie améliore la gestion de l'identité et la gestion de l'identité à la frontière sert la sécurité nationale. Comme nous l'avons évoqué à la section IV, l'élargissement de la collecte et

²⁴⁹ Liberty Human Rights, « Legal Challenge: Ed Bridges v. South Wales Police », sans date. Consultation le 11 août 2021. <https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/>.

²⁵⁰ *Supra* note 246.

de l'utilisation de données biométriques, plus particulièrement après les attentats du 11 septembre, a été motivé par leurs avantages présumés en matière de sécurité nationale.

168. Il reste que **la sécurité nationale comme justification principale des activités biométriques a pâli avec le temps au regard d'autres objectifs.**
169. Parmi ceux-ci on compte d'abord les avantages plus vastes associés à la gestion de l'identité, qu'il s'agisse de l'évaluation de l'admissibilité et des droits, de la prévention de la fraude ou des gains d'efficacité dans la prestation des services. Il convient de noter que, à l'heure actuelle, l'ASFC et IRCC ne définissent pas avant tout en termes de sécurité nationale leurs activités biométriques bien établies. Le but du Programme de passeport est de permettre aux Canadiens admissibles de voyager et le but du Programme d'immigration est de gérer le flux d'étrangers venant au pays, dont la grande majorité ont des raisons légitimes de vouloir y entrer. Les données biométriques sont des renseignements sur les gens qui facilitent ces fonctions. Dans chaque cas, les avantages pour la sécurité nationale sont la conséquence d'une solide gestion de l'identité à laquelle contribue la biométrie²⁵¹. Plus récemment, la facilitation des mouvements des voyageurs s'est imposée avec des programmes et des projets pilotes intégrant la biométrie et la technologie mobile dans la recherche de mouvements « sans contact » et « sans congestion » (ce dernier aspect offrant un intérêt tout particulier en période de COVID-19).
170. La biométrie va au-delà du domaine de la sécurité nationale, mais les résultats qu'elle permet à ce chapitre sont indéniables. La gestion de l'identité consiste en partie à identifier les gens malveillants, y compris les terroristes, les voyageurs extrémistes canadiens et les autres menaces pour la sécurité nationale et internationale. Le contrôle biométrique dans le cas, par exemple, des demandes d'immigration ou de passeport comprend une recherche dans les bases de données (nationales et étrangères) qui peuvent renvoyer des renseignements d'intérêt pour la sécurité nationale (présence sur une liste de surveillance, activité terroriste suspecte, condamnations antérieures pour atteinte à la sécurité nationale, cumul d'identités, etc.).
171. L'évaluation de la proportionnalité de ces programmes doit donc se faire à la lumière de l'ensemble des avantages pour les activités du Canada à la frontière qui découlent de la biométrie. Cela comprend les avantages pour la gestion de l'identité dans les décisions d'admissibilité et d'octroi de passeport, le contrôle des voyageurs et la sécurité nationale.
172. Le continuum frontalier décrit dans la présente étude met en évidence plusieurs éléments sur lesquels l'OSSNR pourrait se pencher à l'avenir :
- Collecte de données biométriques dans les centres de réception de demandes de visa (CRDV). À cet égard, le problème de sécurité nationale qui se pose tient aux renseignements personnels – et aux données biométriques – qui passent par les CRDV exploités dans des territoires à haut risque et gérés par des entrepreneurs privés et des sous-traitants. Un examen des CRDV viserait non seulement les risques liés à la collecte et à la communication des renseignements biométriques, mais aussi les dispositions plus générales en matière de sécurité et les conséquences du fonctionnement général de ces centres sur la sécurité nationale.

²⁵¹ Ainsi, les demandes frauduleuses de passeport peuvent être découragées ou détectées; les étrangers présentant un risque pour la sécurité peuvent être dissuadés de présenter une demande pour venir au Canada ou, s'ils le font, être reconnus par leurs données biométriques, ce qui entraînera le refus de leur demande.

- Cas où la biométrie permet de relier des renseignements entre des bases de données à des fins de sécurité nationale. Par exemple, quelles sont les statistiques et autres paramètres liés aux résultats au chapitre de la sécurité nationale lorsque des recherches automatisées sont effectuées dans les bases de données des partenaires du M5 dans le contexte de l'immigration (p. ex. renseignements menant à une décision d'interdiction de territoire pour les raisons mentionnées à l'article 34 de la LIPR). Qu'en est-il des échanges au cas par cas avec ces partenaires et d'autres motivés par des préoccupations en matière de sécurité nationale? Quel rôle ont pu jouer les renseignements biométriques dans les cas où le ministre de la Sécurité publique a refusé, révoqué ou annulé un passeport canadien pour des raisons de sécurité nationale? Ces exemples illustrent les possibilités d'examen des activités de sécurité nationale que rend *possibles* la biométrie. Dans de tels cas, la recherche d'un équilibre entre confidentialité et sécurité – entre la protection des renseignements personnels de nature délicate et les objectifs de sécurité de l'État – fait clairement ressortir le rôle que peut jouer l'OSSNR en examinant le caractère légitime, raisonnable et nécessaire de ces activités.
- Autres situations où les données biométriques recueillies à une certaine fin sont utilisées par la suite dans un autre programme ou à d'autres fins (voir l'analyse du double usage aux paragraphes 191 à 201 plus loin).

2. Activités établies

173. Dans l'ensemble, les activités biométriques établies du gouvernement du Canada dans le continuum frontalier sont bien appuyées actuellement par des pouvoirs conférés par la loi et sont conformes à la pratique internationale.
174. L'utilisation de la biométrie par IRCC et l'ASFC dans leurs programmes établis est bien fondée et autorisée par des dispositions détaillées de la loi. La prise et la vérification d'empreintes digitales et de photos faciales par le Canada dans le contexte de l'immigration sont également conformes à ce que font les autres membres du M5²⁵². Dans sa conception, l'utilisation de données dactyloscopiques facilite les échanges de renseignements avec les partenaires du M5 qui font la même collecte dans le cadre de leurs propres programmes et de leurs lois nationales de l'immigration²⁵³.
175. De même, le passeport électronique canadien respecte les normes établies par l'Organisation de l'aviation civile internationale (OACI), qui impose le recours à la photographie faciale comme mesure biométrique. Dans le monde, plus de 140 pays ont adopté le passeport électronique selon les spécifications de l'OACI, ce qui rend le système interopérable et facilite les déplacements internationaux des titulaires de passeports canadiens. Le recours à la reconnaissance faciale dans le processus de demande de passeport respecte les lignes directrices de l'OACI et les pratiques exemplaires en matière de délivrance de documents de voyage.

²⁵² IRCC, « Evaluation of the Biometrics (Steady State) », OSSNR_202002_005.

²⁵³ ASFC, « Biometrics Collection for Immigration Purposes M5 Comparison », sans date [OSSNR_202002_039].

176. Le cadre législatif des activités établies confère des bases solides à la collecte, à l'utilisation, à la conservation et à la communication de données biométriques dans le cadre du Programme d'immigration et du Programme de passeport du gouvernement du Canada. Il n'en subsiste pas moins des préoccupations précises dont nous allons parler.

3. Recours élargi à la biométrie avec le temps

177. **Le recours à la biométrie dans le continuum frontalier a considérablement augmenté depuis 30 ans, et il est probable qu'il continue à progresser. Cette tendance a en partie pour moteur l'avancement des capacités technologiques et l'évolution des défis en matière de gestion de l'identité.**
178. Concernant d'abord, en 1993, les demandeurs d'asile et les personnes expulsées, la collecte de données biométriques s'est étendue à tous les étrangers sans dispense qui entrent au pays et, par le Programme de passeport, à tous les citoyens canadiens, les résidents permanents et les réfugiés qui demandent respectivement un passeport, un certificat d'identité et un document de voyage pour réfugiés²⁵⁴. Le Projet d'expansion de la biométrie a vu le jour dans le but exprès d'accroître la portée – collecte, partage et utilisation – de la biométrie. Les partenaires du M5 se réunissent régulièrement en groupes de travail pour peaufiner et renforcer (et fréquemment aussi pour élargir) l'information sur l'immigration qu'ils partagent. Dans des projets pilotes et des travaux de recherche menés ces quelques dernières années, on a examiné l'utilisation de la technologie de reconnaissance faciale dans les aéroports. Dans d'autres, on a étudié l'intégration de la technologie mobile à la gestion de l'identité biométrique dans le continuum des voyages.
179. Nul doute que le développement technologique explique une partie de cet élan. Nous *pouvons* faire plus, et c'est ce que nous faisons. Tirer parti des nouvelles capacités pour améliorer l'exécution des programmes est un objectif légitime. Il faut savoir en revanche que le déterminisme technologique ne saurait justifier en soi la collecte de renseignements sensibles. Les nouvelles activités biométriques trouveront leur justification dans le caractère nécessaire et proportionné de la collecte et de l'utilisation de données biométriques à des fins voulues.
180. Un autre facteur qui joue est le désir de suivre le rythme des autres administrations. Comme les pays du monde élargissent leurs activités biométriques, il va de soi que le Canada fasse de même, facilitant ainsi les voyages à l'étranger pour les Canadiens, rendant plus faciles aux non-Canadiens les déplacements vers et à travers le Canada et aidant les représentants du pays à constater les risques possibles pour la sécurité (notamment grâce à l'échange d'information avec le M5). Pourtant, désirer demeurer en phase avec autrui, même avec les proches partenaires internationaux du Canada, n'est pas en soi une justification valable pour une extension de la collecte et de l'utilisation de renseignements personnels de nature délicate. Là encore, chaque activité nouvelle doit être évaluée et justifiée indépendamment.
181. **Exploiter les possibilités engendrées par l'évolution technologique et vouloir suivre le rythme des autres administrations ne peuvent justifier en soi un recours plus large à la biométrie. Cette**

²⁵⁴ Si des photographies sont prises depuis des décennies dans le cadre des demandes de passeport, IRCC n'applique que depuis 2010 la Solution de reconnaissance faciale qui fait de la photographie de passeport une pièce biométrique; ajoutons que, de même, le passeport électronique n'est devenu la norme qu'en 2013.

justification doit être fonction du caractère nécessaire et proportionné de la collecte et de l'utilisation de données biométriques à des fins particulières voulue.

4. Projets pilotes

182. Les projets et les initiatives pilotes soulèvent plus de préoccupations que les activités établies, car ils risquent d'être réalisés à titre expérimental sans assises suffisantes dans les lois ou les politiques. Ces projets sont un sujet d'intérêt constant pour l'OSSNR.
183. Les projets pilotes sont des véhicules pour avancer, une tribune pour de nouvelles techniques et technologies susceptibles de mettre à mal l'équilibre proportionnel entre les objectifs du gouvernement et les atteintes à la vie privée. Ajoutons que, en règle générale, les Canadiens ont accès à moins de renseignements publics sur les activités pilotes. Dans notre rapport, nous décrivons plusieurs de ces projets, bien que, compte tenu de l'accent que nous mettons sur les activités en cours, notre propos ne soit pas de déterminer si un projet pilote quelconque est proportionné dans sa collecte et son utilisation de données biométriques.
184. On verra néanmoins dans le projet Visages en mouvement (FOTM) une illustration des défis et des préoccupations propres aux projets pilotes. Le projet pilote en question s'appuyait sur une autorité législative conférée par les articles 15 à 18 de la LIPR et pourtant, ces dispositions avaient été rédigées avant même que la technologie de la reconnaissance faciale ne soit envisagée. L'OSSNR n'a pas la conviction que les articles 15 à 18 de la LIPR autorisent nettement la collecte de données biométriques faciales des voyageurs, plus particulièrement avant l'arrivée au point de contrôle officiel et après le passage de ce dernier. On devrait dès lors solliciter des avis juridiques pour être sûr que de telles activités sont bien fondées sur les pouvoirs conférés par la loi à l'ASFC et qu'elles sont conformes aux exigences de l'article 8 de la Charte. On doit aussi prêter attention à la politique-cadre régissant les activités pilotes, de sorte que les renseignements personnels en cause soient dûment caractérisés. On devrait également par des énoncés de confidentialité et un affichage public assurer une transparence appropriée pour le public en ce qui concerne le déploiement de nouvelles technologies et les fins de leur application.
185. Les projets pilotes qui donnent lieu à une collecte de renseignements privés ou personnels doivent recevoir une attention suffisante sur le plan des lois et des politiques²⁵⁵. L'OSSNR s'attend à ce que les ministères se livrent, malgré le caractère provisoire ou expérimental d'un projet, à une analyse nécessaire pour garantir que la loi confère le pouvoir de mener l'activité en question et que la collecte, l'utilisation, la conservation et la communication de renseignements personnels qui en découlent sont bien régies par des politiques.

²⁵⁵ Ainsi, le rapport final sur le projet FOTM dit : [traduction] « Les protocoles de confidentialité et de sécurité applicables aux caméras de surveillance sont bien établis en ce qui concerne la notification, la visualisation, l'utilisation, le stockage et l'élimination. L'avènement de l'identification assistée par machine peut nécessiter une extension des protocoles actuels. » (Nous soulignons.) Face4 Systems Inc., « Face4 Final Report For CSSP Project CSSP – 2014 », p. 2 [OSSNR_202002_072, p. 2].

5. Évolution des normes juridiques et sociétales

186. Le débat public sur les pouvoirs conférés par la loi cherche à déterminer si les normes et les protections existantes sont suffisantes pour réglementer les activités biométriques ou si de nouvelles normes et protections sont nécessaires.
187. Ce débat prend de l'ampleur, surtout en ce qui concerne la technologie de reconnaissance faciale. Les données biométriques sont des renseignements personnels, mais elles ont des traits qui peuvent les distinguer; elles rendent compte de caractéristiques personnelles immuables, elles permettent une identification fiable à distance et elles servent d'identificateurs uniques susceptibles d'être utilisés pour découvrir des renseignements sur des personnes et établir des liens entre plusieurs ensembles de données. La question est de savoir s'il convient de traiter la biométrie comme une information compatible avec les autres renseignements personnels recueillis par le gouvernement dans le cadre de ses programmes et de ses activités. Des régimes juridiques précis sont-ils nécessaires pour créer des normes qui traduisent bien le caractère potentiellement intrusif et délicat de certaines données biométriques, et devrait-il y avoir des limites d'utilisation particulières au-delà de celles qui s'appliquent actuellement en vertu de la *Loi sur la protection des renseignements personnels*²⁵⁶?
188. Le Commissariat à la protection de la vie privée du Canada (CPVP) a fait part de ses observations sur cette question dans le contexte de sa récente enquête sur l'utilisation par la GRC de la reconnaissance faciale par l'entremise de l'entreprise privée Clearview-AI. « Les lois canadiennes sur la protection des renseignements personnels ont été conçues de manière à être neutres sur le plan technologique », a écrit le CPVP, « ce qui est une bonne chose, compte tenu du rythme des changements technologiques par rapport au rythme des travaux nécessaires pour moderniser les lois. Toutefois, les risques que présente la technologie de RF [reconnaissance faciale] sont tels que des règles particulières pourraient s'avérer justifiées en raison du caractère inaltérable de l'information en cause²⁵⁷. » Le rapport souligne en outre que de nombreux pays ont élaboré des lois de protection de la vie privée qui réglementent en particulier les activités biométriques. À l'heure actuelle, le Québec est la seule province canadienne à avoir adopté une loi traitant expressément de la biométrie²⁵⁸. D'autres pays réclament ou imposent une interdiction pure et simple des technologies de reconnaissance faciale²⁵⁹. Le contrôleur européen de la protection des données, par exemple, a appelé à l'interdiction de la reconnaissance faciale

²⁵⁶ Commissariat à la protection de la vie privée, « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée ».

²⁵⁷ Commissariat à la protection de la vie privée, « Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée ».

²⁵⁸ *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, ch. 32, articles 44 et 45. Voir cette loi *in extenso* à <http://www.legisquebec.gouv.qc.ca/fr/document/lc/C-1.1?&cible=>. Voir aussi Commission d'accès à l'information du Québec, « Biometrics: Principles and Legal Duties of Organizations », juillet 2020. Consultation le 8 octobre 2021. https://www.dataguidance.com/sites/default/files/cai_g_biometrie_principes-application_eng.pdf.

²⁵⁹ Voir *supra* note 246.

dans les lieux publics, soutenant que de telles applications constituent [traduction] « une ingérence profonde et non démocratique dans la vie privée des individus²⁶⁰ ».

189. Les organismes de défense des libertés civiles ont exprimé haut et fort leurs préoccupations au sujet des activités biométriques, tout comme les milieux universitaires et les médias. Par ailleurs, les gouvernements peuvent mettre à profit les nouvelles capacités et les nouveautés dans la réalisation de leurs objectifs de programme, mais doivent respecter en même temps les droits fondamentaux de la personne. On connaît bien la tension au cœur de ce débat – comment parvenir aux objectifs gouvernementaux avec efficacité et efficacie, tout en protégeant la vie privée des gens? C'est une tension qui se manifeste plus généralement dans les activités d'intérêt pour la sécurité nationale, la société opposant la sauvegarde des droits individuels et la protection de la collectivité. Dans le présent contexte, ce dilemme éternel est catalysé par des avancées technologiques qui élargissent à la fois la trousse d'outils du gouvernement et les possibilités d'atteinte à la vie privée, plus particulièrement dans la collecte et l'utilisation de données personnelles de nature délicate. Dans l'avenir, la question de savoir comment les activités biométriques sont conçues, mises en œuvre et réglementées sera en partie déterminée par l'évolution des normes de la société, les principes juridiques établis (avec les considérations relatives à la *Charte*) et les valeurs canadiennes de longue date que sont la démocratie et les droits de la personne.

190. Bien que la frontière soit comparativement un espace où une plus grande intrusion est jugée raisonnable, une telle justification n'est pas illimitée et devra être soigneusement dosée. Pour l'OSSNR comme pour d'autres organismes d'examen, l'évolution des normes juridiques et sociétales déterminera comment des considérations comme le caractère conforme et raisonnable devraient s'appliquer.

6. Double usage de la biométrie

191. Par double usage, on entend une utilisation de données biométriques à d'autres fins que celles pour lesquelles elles ont été recueillies ou dans un autre programme que celui pour lequel elles l'ont été. Cela repose sur une certaine logique. La biométrie constitue une solide source d'information sur les gens; si elle est utile dans un contexte, elle le sera sans doute dans un autre. Toutefois, cette dynamique constitue une grande source de préoccupations en matière de vie privée²⁶¹.

192. L'OSSNR a relevé plusieurs cas de double usage possible des renseignements biométriques dans les activités sur lesquelles porte son rapport.

193. Premièrement, les photos prises dans le cadre du Programme de passeport servent aussi à la mise en correspondance faciale pour le programme NEXUS.

²⁶⁰ Contrôleur européen de la protection des données, « Artificial Intelligence Act: A welcome initiative, but ban on remote biometric identification in public space is necessary », communiqué, 23 avril 2021. Consultation le 19 août 2021. https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_fr.

²⁶¹ Voir les apports à Patrizio Campisi (dir.) *Security and Privacy in Biometrics* (Springer : Londres, 2013) pour des exemples tirés des études spécialisées.

194. Deuxièmement, les organismes d'application de la loi ont, dans le cadre de leurs enquêtes, accès aux empreintes digitales des étrangers prises dans le cadre des demandes d'immigration. Si la GRC conserve les données dactyloscopiques pour l'immigration et la criminalité dans des répertoires distincts, les deux sont consultés lorsque les forces de l'ordre soumettent des empreintes digitales à des fins d'identification.
195. Troisièmement, le SCRS, la GRC et l'ASFC peuvent communiquer des photos à IRCC à des fins de contrôle par reconnaissance faciale avec les photos de demande de passeport ou de documents de voyage. La chose est possible dans le contexte des enquêtes de sécurité nationale ou d'application de la loi s'il s'agit d'identifier un inconnu, d'établir si une personne a plusieurs identités ou d'aider à exécuter un mandat.
196. Le double usage ne pose pas toujours un problème de conformité. En fait, de nombreux usages doubles sont bien fondés en droit si on considère la norme des « usages compatibles » à l'alinéa 8(2)a) de la *Loi sur la protection des renseignements personnels*, la faculté qu'ont certaines institutions de solliciter des renseignements personnels en vertu de l'alinéa 8(2)e) de la même loi ou l'application d'autres dispositions législatives à caractère sectoriel (voir, par exemple, les paragraphes 63, 109 et 112 qui décrivent les autorisations des usages qui précèdent dans le domaine de l'exécution de la loi). Dans le cas de NEXUS en particulier, l'utilisation des photos de passeport est nettement un usage compatible (voir le paragraphe 140). Les préoccupations en matière de protection de la vie privée se font encore plus discrètes si les programmes sont volontaires ou qu'on obtient le consentement des gens au préalable.
197. **Cependant, même lorsqu'elles présentent des avantages démontrables, les nouvelles utilisations des données biométriques recueillies doivent être soigneusement examinées pour en garantir le caractère raisonnable et proportionné. De plus, tous les nouveaux usages doivent être justifiés et autorisés par la loi.**
198. Bien qu'autorisées par la loi, les situations où les données biométriques recueillies dans le continuum frontalier sont exploitées à des fins autres (là où, par exemple, les organismes d'enquête se servent de renseignements biométriques initialement recueillis aux fins de l'immigration ou de la délivrance de passeports) méritent qu'on s'y attarde. L'OSSNR pourrait revenir sur ces cas lorsqu'il envisagera un futur examen d'activités biométriques.
199. **Disons enfin que le principe de la « limitation de la finalité » peut être le moyen de se garder de tout double usage injustifié dans le cadre des activités biométriques²⁶².**
200. Il y a limitation de la finalité si on mentionne en termes exprès la finalité bien précise de l'utilisation des données biométriques recueillies en s'engageant à ne pas les utiliser dorénavant à d'autres fins²⁶³. Ce principe est bien ancré dans la jurisprudence britannique et européenne et est plus restrictif que l'« usage compatible ». Le principe des « usages compatibles » reflète un engagement permanent pris par le gouvernement du Canada de limiter l'application des

²⁶² Information Commissioner's Office (Royaume-Uni), « Principle (b): Purpose limitation », sans date. Consultation le 12 août 2021. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/?q=DPIA>.

²⁶³ Information Commissioner's Office (Royaume-Uni), « Principles », sans date. Consultation le 12 août 2021. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>.

renseignements personnels à d'autres fins; la norme doit être interprétée le plus étroitement possible pour ce qui est des renseignements biométriques. Répétons que les identificateurs biométriques sont uniques comparativement aux autres identifiants personnels parce que, pour l'essentiel, ils sont permanents et immuables²⁶⁴. Cela signifie que, une fois qu'ils sont obtenus sans être nettement assujettis à des politiques de conservation-suppression et à des limitations de la finalité, le gouvernement a sous la main un répertoire de renseignements permettant d'identifier les gens à l'avenir – peut-être dans le cadre d'activités moins anodines que les activités au titre desquelles les données biométriques ont été recueillies au départ²⁶⁵.

201. Il serait prématuré pour l'OSSNR de conclure ou non au caractère raisonnable ou proportionné des cas possibles de double usage que nous venons d'évoquer. Lui ou un autre organisme d'examen pourrait se pencher plus à fond sur la question dans une future étude.

7. Systèmes techniques

202. L'OSSNR a passé en revue les renseignements techniques généraux sur les activités sur lesquelles porte son étude. Cela comprend des données sur les divers systèmes et bases de données exploités dans le cadre des activités biométriques du gouvernement du Canada.
203. **Il existe un important chevauchement entre les bases de données et les systèmes techniques utilisés dans l'ensemble des activités biométriques établies.**
204. Le Programme de passeport et le Programme d'immigration utilisent tous deux le Système mondial de gestion des cas (SMGC)²⁶⁶ et IRCC, l'ASFC et la GRC ont accès à ce système²⁶⁷. Dans le contexte de l'immigration, les photos faciales sont versées dans le SMGC, tandis que les empreintes digitales sont envoyées à la GRC et stockées dans un des répertoires (celui de

²⁶⁴ Le *Règlement général sur la protection des données* (RGPD) de l'Union européenne dit que les renseignements biométriques forment une « catégorie particulière de données » (article 9) en raison de leur sensibilité. (Voir le règlement *in extenso* à <https://gdpr-expert.eu/article.html?id=9#textesofficiels>). La *Loi générale sur la protection des données du Brésil* établit des catégories semblables à l'article 5 (voir cette loi *in extenso* à https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf). Il en va de même de l'Inde avec son projet de *Loi sur la protection des données personnelles* (article 3, alinéa 36) (voir ce projet de loi *in extenso* à https://prsindia.org/files/bills_acts/bills_parliament/Personal%20Data%20Protection%20Bill,%202019.pdf).

²⁶⁵ On peut penser, par exemple, à la National Database and Registration Authority (NADRA) au Pakistan. Créée en l'an 2000 en vue de moderniser l'enregistrement des cartes d'identité, la base d'information NADRA a par la suite servi à combattre le terrorisme en relation avec l'enregistrement des cartes SIM ainsi qu'à appliquer la technologie de la reconnaissance faciale par caméra en circuit fermé dans plusieurs grandes villes de ce pays. Voir Privacy International, « Identity Policies : The Clash Between Democracy and Biometrics », 30 janvier 2018. Consultation le 19 août 2021. <https://privacyinternational.org/long-read/1100/identity-policies-clash-between-democracy-and-biometrics>.

²⁶⁶ Si le Programme de passeport utilise avant tout le Système intégré de récupération d'information (IRIS), IRCC a indiqué à l'OSSNR qu'il [traduction] « est en cours de transition [de IRIS] au [SMGC] » en commençant par les passeports diplomatiques et spéciaux, les documents de voyage pour réfugiés et les certificats d'identité. Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 5.

²⁶⁷ Protocole d'entente IRCC-ASFC de 2017, paragraphe 8.4 de l'Annexe sur l'échange d'information.

l'immigration) du Système automatisé d'identification dactyloscopique (SAID). Ce répertoire est alors consultable par les organismes d'application de la loi au pays et peut être interrogé par les pays partenaires du M5 aux fins de l'immigration.

205. Par ailleurs, les demandes de passeports et de documents de voyage dans le cadre du Programme de passeport sont versées à la fois dans le SMGC et le fichier central d'IRCC (voir l'Annexe A. Note technique : Systèmes du Programme d'immigration et du Programme de passeport), mais IRCC a fait savoir qu'un passage intégral au SMGC est prévu pour les années à venir²⁶⁸. La photo numérisée de la demande est envoyée à la Solution de reconnaissance faciale (SRF) d'IRCC, convertie en modèle biométrique, transmise pour évaluation à la base de données de la SRF et stockée dans le fichier central. Tant dans le Programme d'immigration que dans le Programme de passeport, on emploie à la réception des demandes – et des données biométriques – un ensemble de systèmes aux différents lieux où des demandes sont présentées dans le monde qui tous sont raccordés aux serveurs d'IRCC au Canada.
206. **L'architecture générale de ce système – collecte, transmission et stockage des données biométriques dans le cadre des activités du gouvernement du Canada dans le continuum frontalier – est complexe sans toutefois poser nécessairement un problème.**
207. Dans l'esprit même de la présente étude, l'OSSNR fait ces observations comme première étape de la cartographie de l'architecture des systèmes applicables. Cette cartographie résumée dans l'Annexe A. Note technique : Systèmes du Programme d'immigration et du Programme de passeport, sera utile à l'OSSNR s'il choisit d'examiner en détail les divers systèmes techniques servant à la biométrie dans les activités frontalières en voulant notamment voir comment ils se chevauchent et quels problèmes de confidentialité ou de sécurité, s'il y en a, pourrait poser la structure en place.

8. Connaissance des algorithmes

208. En plus des préoccupations publiques déjà évoquées au sujet de la surveillance gouvernementale, il existe des appréhensions connexes au sujet d'une prise de décisions automatisée ou assistée par automate, plus particulièrement en relation avec l'identification biométrique²⁶⁹. L'inquiétude générale que suscitent les algorithmes et l'automatisation a pour objet l'opacité de la prise de décisions, même pour les opérateurs humains qui s'appuient sur les algorithmes ou les systèmes en question pour faire leur travail²⁷⁰.
209. **Dans le Programme d'immigration et le Programme de passeport et aux bornes d'inspection primaire, IRCC, l'ASFC et la GRC n'ont qu'une connaissance limitée de la façon dont fonctionnent les algorithmes employés.**
210. Ces algorithmes viennent de fournisseurs privés et les détails de leur mode de fonctionnement relèvent de l'exclusivité. En ce sens, ils sont essentiellement une « boîte noire ». L'OSSNR préconise une plus grande transparence du mode de fonctionnement des algorithmes

²⁶⁸ Réponse écrite d'IRCC à l'OSSNR, 4 décembre 2020, p. 5.

²⁶⁹ Israel, « Facial Recognition at a Crossroads », p. 61.

²⁷⁰ Israel, « Facial Recognition at a Crossroads », p. 61.

qui analysent les renseignements personnels. La transparence est nécessaire pour que des tiers puissent vérifier la fidélité et la fiabilité des algorithmes. La confiance du public s'en trouverait renforcée tant pour la capacité des algorithmes à fonctionner en toute équité et sans discrimination que pour celle des ministères à remédier à toute lacune à cet égard.

211. **Chaque ministère ou organisme a toutefois bel et bien démontré que des mesures de rendement (sous forme, par exemple, de taux d'erreur) sont connues et éprouvées et que des adaptations (de seuils de correspondance, par exemple) se font au besoin.**
212. De plus, dans le cas de la SRF d'IRCC et du SAID de la GRC, il y a intervention humaine tant pour vérifier les résultats du système que pour effectuer des comparaisons au besoin. En revanche, la mise en correspondance faciale aux bornes d'inspection primaire se fait sans qu'un jugement humain soit porté, quoiqu'il soit loisible aux ASF de corriger par la suite toute erreur évidente par une vérification visuelle.

9. Prévention des biais et de la discrimination

213. À l'opacité des algorithmes se conjugue le risque qu'une analyse biométrique automatisée – reconnaissance faciale, comparaison d'empreintes digitales, etc. – soit entachée d'un biais. Il est bien documenté dans les études spécialisées, par exemple, que les algorithmes de reconnaissance faciale sont nombreux à identifier moins sûrement les femmes, les personnes très jeunes ou très âgées et les gens au teint plus basané²⁷¹. De même, la prise et la comparaison des empreintes digitales peuvent se révéler plus difficiles et/ou moins précises pour les femmes, certains groupes ethniques et les gens de certains métiers (ce qui peut être le reflet de la situation socioéconomique)²⁷². La possibilité d'un biais systématique est préoccupante si on considère que d'importantes décisions dans le continuum frontalier sont fondées sur l'analyse automatisée, qu'il s'agisse de la délivrance de documents de voyage officiels, de l'octroi de visas, de l'asile ou de la résidence ou d'un éventuel aiguillage en vue d'obtenir un complément d'information ou de pousser plus loin l'inspection pendant le processus d'immigration et de dédouanement.
214. **IRCC et l'ASFC ont examiné dans des analyses préliminaires les répercussions possibles de leurs activités biométriques sur divers groupes, bien que l'application d'éventuelles stratégies d'atténuation ne soit pas toujours évidente.**
215. Dans l'ACS+ consacrée en mai 2016 aux BIP par exemple, il a été proposé que l'Agence applique des seuils de correspondance faciale spécifiques aux hommes et aux femmes; une analyse d'octobre 2020 sur un biais possible selon le sexe dans les BIP a donné lieu à une

²⁷¹ NIST, « Face Recognition Vendor Test (FRVT) Part 3 », <https://doi.org/10.6028/NIST.IR.8280>. Voir aussi Alice O'Toole et coll., « Demographic effects on estimates of automatic face recognition performance », *Image and Vision Computing*, mars 2012, 30 (3): 169-176; voir aussi Nicholas Furl et coll., « Face recognition algorithms and the other-race effect: Computational mechanisms for a developmental contract hypothesis », *Cognitive Science*, Novembre-décembre 2002, 26 (6): 797 à 815.

²⁷² P. Drozdowski et coll., « Demographic Bias in Biometrics ». Voir aussi Hicklin et Reedy, « Implications of the IDENT/IAFIS Image Quality ».

recommandation semblable. Dans le cas de la reconnaissance faciale tant pour la SRF (IRCC) que pour les BIP (ASFC), de récents tests de rendement ont permis d'étudier directement la possibilité d'un biais démographique. L'analyse a relevé de légères inégalités de précision selon le sexe, mais en faisant valoir que les améliorations apportées avec le temps (mise à jour des algorithmes) ont permis une réduction constante de ces inégalités sans les éliminer.

216. **Dans certains contextes, le progrès technologique a aidé à réduire – sans les éliminer – les différences au chapitre des répercussions.**
217. Il reste à faire le travail nécessaire – au-delà de la constatation de ces petits écarts – pour apporter une solution complète à ces problèmes. L'ASFC a fait observer, par exemple, que son [traduction] « travail dans ce domaine commence à peine sans encore rien de concluant et avec encore beaucoup de travail à faire²⁷³ ». Cela comprend une ACS+ sur les technologies de reconnaissance faciale, une étude de la visibilité des biais dans les données et l'élaboration d'éventuelles mesures d'atténuation sur le plan des politiques²⁷⁴. De même, IRCC a déclaré que [traduction] « de nouvelles évaluations du biais démographique [...] auraient lieu » après l'implantation d'un nouvel algorithme dans la SRF²⁷⁵.
218. Nous ne suggérons pas que les mesures d'atténuation des biais possibles ont été insuffisantes à ce stade, mais plutôt qu'IRCC aussi bien que l'ASFC ont démontré être conscients des problèmes possibles et s'engager à poursuivre le travail dans ce domaine. Toutefois, de tels efforts ne devraient pas se limiter à des tests de précision ni à des améliorations d'algorithmes. On devrait aussi envisager des solutions sur le plan des politiques comme l'application des stratégies d'atténuation déjà indiquées et l'analyse des conséquences possibles des erreurs biométriques dans l'expérience des gens touchés.
219. Si on veut s'assurer d'un futur usage raisonnable des algorithmes en question, on doit s'engager à continuer de réduire les inégalités entre groupes causées par leur fonctionnement et à veiller à ce que, dans les décisions humaines qui suivent le contrôle biométrique, de telles différences soient prises en compte.
220. **On se doit de poursuivre le travail si on veut atténuer les répercussions différentes sur les divers groupes dans la population. Toutefois, les ministères et organismes examinés dans notre étude ont démontré être conscients des inégalités systémiques possibles et se sont engagés à y mettre fin.**

8. Conclusion

221. La biométrie joue un rôle fondamental dans le continuum frontalier. Le gouvernement du Canada recourt à la biométrie pour vérifier et établir l'identité des personnes avec pour conséquence qu'on peut répondre avec plus d'assurance à la question de savoir qui entre au

²⁷³ Réponse écrite de l'ASFC à l'OSSNR, 4 février 2021, « Annex 5 - Travellers Branch (PIK & SFV) », p. 3.

²⁷⁴ Réponse écrite de l'ASFC à l'OSSNR, 1^{er} octobre 2021.

²⁷⁵ Réponse écrite d'IRCC à l'OSSNR, 3 août 2021, p. 4.

pays et s'il a le droit d'y entrer. Dans le contexte de l'immigration, cela signifie le contrôle, la vérification (à l'arrivée) et l'évaluation continue de l'admissibilité des étrangers qui viennent au Canada à titre de résidents temporaires ou permanents. On contrôle les demandeurs de passeports canadiens (et d'autres documents officiels de voyage) pour confirmer l'admissibilité aux services de passeport et le droit à un passeport et on utilise ensuite leurs données biométriques intégrées au passeport électronique à l'occasion de leurs voyages à l'étranger. Ces deux activités convergent aux aéroports canadiens où l'ASFC vérifie l'identité des voyageurs par reconnaissance faciale aux bornes automatisées.

222. Notre but dans cette étude était d'examiner et de contextualiser les activités en question. Nous avons jeté un regard en arrière et remonté le cours de l'évolution des activités biométriques du gouvernement du Canada dans le continuum frontalier en observant un passage d'objectifs strictement axés sur la sécurité nationale à des buts plus larges de gestion de l'identité. Nous avons aussi regardé vers l'avenir et considéré de futures applications biométriques possibles, dont l'adoption de l'identité numérique, voire une plus grande systématisation de la biométrie à l'échelle de l'expérience du voyageur.
223. Nos observations sont destinées tant au public canadien lorsqu'il se penche sur la collecte et l'utilisation de renseignements biométriques par le gouvernement qu'à l'OSSNR lorsqu'il planifie de futurs examens dans ce domaine. Nous avons remarqué que les activités établies sont bien appuyées par des pouvoirs conférés par la loi et qu'elles sont conformes à la pratique internationale. Par ailleurs, certains aspects peuvent susciter des préoccupations. On peut notamment penser aux projets pilotes, qui servent à mettre des concepts à l'essai et exigent un examen juridique attentif, à la constante possibilité d'inégalités systémiques entre divers groupes dans l'analyse faite par les algorithmes biométriques, et au double usage éventuel des renseignements biométriques du fait de l'accessibilité de cette information pour les organismes d'enquête.
224. Le débat public sur l'usage que fait le gouvernement de la technologie biométrique continuera à évoluer et orientera l'évolution de l'encadrement de ces activités par les lois et les règlements. Il y a lieu en soi de poursuivre notre examen, plus particulièrement là où la collecte et l'utilisation des données biométriques sont justifiées par des mentions expresses de leurs résultats en matière de sécurité nationale.



Inventaire et description des systèmes

OSSNR // Étude de l'utilisation de la biométrie par le gouvernement du Canada dans le continuum frontalier 79

SMGC	IRCC	IRCC, ASFC, GRC	Système mondial de gestion des cas (SMGC)	COSMOS
SAID	GRC	IRCC, ASFC, GRC	Système automatisé d'identification dactyloscopique (SAID)	SITR, CIPC, NCIC
SCIBI	IRCC	IRCC, ASFC	Système canadien d'identification biométrique aux fins d'immigration (SCIBI)	
DLEE	IRCC	ASFC, Service Canada, CRDV	Dispositif de lecture électronique des empreintes digitales (DLEE)	SCIBI
LiveScan	ASFC	ASFC	Appareil de lecture et de transmission électroniques des empreintes digitales. De plus, LiveScan permet une recherche biométrique dans les bases de données criminelles des États-Unis (IAFIS du FBI). On peut passer par les données de vérification de casier judiciaire pour confirmer un résultat du NCIC (recherche biographique dans le système américain de données criminelles).	IAFIS du FBI
IIPV	ASFC	ASFC, TC	Information interactive préalable sur les voyageurs (IIPV)	
PFVFT	ASFC	ASFC	Prise d'une photographie du visage à la frontière terrestre (PFVFT)	SCIBI, SAID
SITR	GRC		Système d'identification en temps réel (SITR)	
TBID	ASFC	ASFC	Base de données sur les identificateurs biométriques des voyageurs (TBID)	SITR
SSOBL	ASFC	ASFC	Système de soutien des opérations dans les bureaux locaux (SSOBL)	
SIAF	ASFC	ASFC	Système d'interdiction et d'alerte à la frontière (SIAF)	SCRS, DPVF, BIP, SLTD d'Interpol

SIED	ASFC	ASFC	Système intégré d'exécution des douanes (SIED)	SCRS, CIPC
NCIC États- Unis	DHS États- Unis	ASFC	National Criminal Information Center aux États-Unis (NCIC)	CIPC, SCIBI

Description fonctionnelle des systèmes

Le **Système mondial de gestion des cas (SMGC)** est le système Web intégré d'IRCC à vocation mondiale qui sert à traiter les demandes d'immigration et de citoyenneté. Il stocke les photographies et les empreintes digitales des demandeurs et permet à IRCC de répondre aux demandes de passeports diplomatiques et spéciaux, de documents de voyage pour réfugiés et de certificats d'identité. Il sert en outre aux échanges de renseignements biométriques entre le Canada et les partenaires du M5 (États-Unis, Australie et Nouvelle-Zélande). Les renseignements biométriques non rattachés à une personne sont conservés dans un « dépôt de données biométriques » géré par IRCC. Il est possible qu'il n'y ait pas de correspondances avec les renseignements biométriques en cas de problème technique ou d'erreur de saisie.

Le **Système automatisé d'identification dactyloscopique (SAID)** est le système de la GRC qui permet de stocker et de comparer les empreintes digitales. Il exploite un algorithme exclusif de fournisseur commercial.

Le **Système canadien d'identification biométrique aux fins d'immigration (SCIBI)** et sa solution de collecte de données biométriques (SCB) sont le principal système de collecte et d'inscription tant des empreintes digitales que des photographies numériques. Outre les données biométriques, le SCIBI enregistre les données biographiques de la page biographique du passeport ou du document de voyage du demandeur.

Le **dispositif de lecture électronique des empreintes digitales (DLEE)** est un dispositif d'enregistrement dactyloscopique permettant de saisir les empreintes digitales pour le SCIBI. Ces appareils utilisés au Canada (dans les centres de Service Canada, par exemple) et à l'étranger dans les centres de réception des demandes de visa doivent fonctionner conformément aux lignes directrices NPS-NIST-ICD 2.1.1 de la GRC. Les fournisseurs qui implantent la solution de vérification systématique des empreintes digitales aux points de collecte doivent respecter ces mêmes lignes directrices.

Les **bornes LiveScan** servent à saisir les images dactyloscopiques, les renseignements biographiques et les photographies numériques des voyageurs. Les renseignements recueillis par les bornes LiveScan sont transmis électroniquement à la GRC par le SISTR à des fins d'identification et de vérification de l'identité des voyageurs. La GRC renvoie les renseignements à la machine et un agent de l'ASFC examine les résultats. Les bornes Livescan peuvent inscrire les empreintes des réfugiés

dans la base de données de l'Immigration au nom d'IRCC et peuvent demander à la GRC de les communiquer manuellement à des systèmes étrangers (le FBI, par exemple).

Le **programme Information interactive préalable sur les voyageurs (IIPV)**, qui a été mis en œuvre en mars 2016, a obligé les transporteurs aériens à fournir des données sur les voyageurs à l'ASFC avant leur départ pour le Canada. L'ASFC renvoie les cas au transporteur aérien en indiquant « embarquement autorisé » ou « embarquement non autorisé » pour chaque voyageur. Ce programme refuse l'embarquement aux voyageurs jugés interdits de territoire au Canada. Le système décrit les exigences particulières que doivent respecter les transporteurs aériens en matière de messages lorsqu'ils soumettent des données de dossiers passagers.

Le **projet de prise d'une photographie du visage à la frontière terrestre (PFVFT)** a été mis à l'essai par l'ASFC et Face4 Systems Inc. afin de recenser et d'évaluer les technologies et les méthodes de captation d'images faciales à travers les pare-brises des véhicules. Le projet vise à améliorer la sécurité à la frontière terrestre grâce à une reconnaissance faciale efficace. Le projet PFVFT a utilisé deux circuits de caméras pour conclure que les deux permettaient une comparaison d'identification collective dans le contexte de la saisie des données à la frontière terrestre.

Le **Système d'identification en temps réel (SITR)** de la GRC gère les répertoires nationaux d'empreintes digitales liées à la criminalité et à l'immigration. Le SITR comprend le Système automatisé d'identification dactyloscopique (SAID), un sous-système de vérification, et un serveur NNS (National Police Services-National Institute of Standards and Technology) (NPS-NIST). Il fonctionne en tandem avec le système de gestion de l'information sur la justice pénale (GIJP). Le serveur NNS gère les demandes soumises au SITR et les réponses de ce dernier. Le serveur GIJP gère les mises à jour de casier judiciaire. Le sous-système de vérification contrôle un ensemble d'empreintes digitales prises au point d'entrée canadien par rapport à l'ensemble obtenu dans le processus de demande à des fins de confirmation d'identité à l'arrivée au pays.

La **base de données sur les identificateurs biométriques des voyageurs (TBID)** permet à l'ASFC de stocker les numéros de référence ID des empreintes digitales de la GRC avec d'autres renseignements d'inscription biométrique tirés des bornes d'inspection primaire pendant le précontrôle des voyageurs.

L'application **Système de soutien des opérations des bureaux locaux (SSOBL)** servait jusqu'en 2014 à recueillir les données biographiques et biométriques des demandeurs aux fins de traitement des demandes d'asile. Les données biographiques étaient stockées dans la base de données du SSOBL et les données biométriques (empreintes digitales) dans la base existante de données sur les réfugiés à la GRC. En 2014, l'application SSOBL a été mise hors service et remplacée par le SMGC (traitement des demandes) et le SCIBI (collecte de données biométriques).

Le **Système d'interception et d'alerte à la frontière (SIAF)** est un système automatisé d'évaluation des risques et de traitement des données sur les voyageurs aux données biométriques inscrites. Le SIAF sert à déterminer l'admissibilité d'une personne par une vérification dans d'autres systèmes et bases de données

comme les listes de surveillance du Service canadien du renseignement de sécurité (SCRS) ou de la base de données SLTD (documents de voyage et d'identité) d'Interpol. Le système fonctionne comme système dorsal de vérification de l'ASFC au service des bornes d'inspection primaire (BIP).

Le **Système intégré d'exécution des douanes (SIED)** est, comme le SIAF, un système dorsal de l'ASFC servant à déterminer l'admissibilité des voyageurs ayant des données biométriques inscrites, en utilisant ses données biographiques dans le cadre d'une vérification des indices comme pour le SIAF et le CIPC.

Le **National Criminal Information Center (NCIC)** du département de la Justice des États-Unis permet à l'ASFC pendant l'inscription biométrique d'établir une correspondance biographique de contrôle de criminalité ou de voir s'il existe déjà des dossiers américains pouvant faire douter de l'identité du demandeur.

Programme de passeport

Le Programme de passeport utilise à la reconnaissance faciale pour juger de l'admissibilité du demandeur à un passeport ou à un document de voyage canadien.

Inventaire et description des systèmes

Inventaire des systèmes aux fins du Programme de passeport				
Nom du système	Propriétaire	Droit d'accès	Description et objet	Interconnexions
IRIS	IRCC	EDSC, AMC	Système intégré de récupération d'information (IRIS)	SMGC, COSMOS
SRF	IRCC	IRCC	Solution de reconnaissance faciale (SRF)	
COSMOS	AMC	IRCC	Système de gestion des opérations consulaires (COSMOS)	IRIS
SMGC	IRCC	IRCC	Système mondial de gestion des cas (SMGC)	COSMOS/PMP, fichier central

Le **Système intégré de récupération d'information (IRIS)** permet au Programme de passeport de gérer les demandes de passeports et de documents de voyage et de délivrer les passeports. Cette activité est en cours de transition vers le SMGC. IRIS en interface avec le Système de personnalisation des passeports électroniques (SPPE), logiciel qui, lors de l'impression des passeports, fournit les renseignements nécessaires pour produire la page biographique principale et insérer les données dans la puce d'identification électronique par radiofréquence (RFID). Le SPPE a été mis au point par la Compagnie canadienne des billets de banque (CBN). IRIS est constitué de trois parties :

Fichier central (FC) : Répertoire principal des dossiers de passeport comprenant les images numérisées des formulaires de demande de passeport et des documents à l'appui.

Travaux en cours (TEC) : Bases de données servant à traiter et à stocker les demandes de passeport en cours de traitement; les données sont renvoyées au fichier central après la production (c'est-à-dire après la délivrance des passeports).

Liste des signalements (LS) : Base de données contenant les données biographiques répertoriées (noms et date de naissance) des gens dont l'admissibilité à un passeport exige un examen ou une enquête supplémentaire en vertu du Décret sur les passeports canadiens.

La **Solution de reconnaissance faciale (SRF)** sert à l'administration du Programme de passeport dans le cas des nouvelles demandes et des renouvellements. Il s'agit d'une technologie d'identification biométrique à des fins de confirmation de l'identité et de détection des fraudes. Cette technologie convertit la photo d'un demandeur en un modèle biométrique numérique en vue d'une comparaison afin de valider l'identité dans une base de données contenant plus de 55 millions de photographies de demandeurs adultes. Les modèles sont stockés dans la base de données de la SRF.

Le fournisseur du logiciel SRF a procuré un guide de l'utilisateur pour la reconnaissance faciale qui décrit les procédures à suivre pour exécuter toutes les tâches du logiciel. Avant d'utiliser le système ou de prendre des décisions d'analyse, les employés d'IRCC doivent suivre avec succès une formation obligatoire du Ministère en comparaison faciale. La Direction générale de la gestion des risques pour l'intégrité (DGGR) d'IRCC, qui est responsable de la SRF, surveille également en permanence l'utilisation, l'accès des utilisateurs, le comportement du système, l'exactitude, les écarts démographiques et les autres questions relatives au système ou aux utilisateurs.

Le **Système de gestion des opérations consulaires (COSMOS)** est la plateforme dont se sert Affaires mondiales Canada (AMC) pour recevoir les demandes de documents de voyage, tout en assurant l'aide consulaire à l'étranger. Les demandes de passeport sont gérées dans le cadre d'un programme de gestion des passeports (PMP) en interface avec le système IRIS d'IRCC pour le transfert des dossiers de cas. Ce module se charge de la réception, du traitement et de l'impression aux fins des demandes de passeport. Seuls les employés ayant obtenu la certification nécessaire en matière de passeports avec l'autorisation d'IRCC peuvent accéder au PMP. Les renseignements biographiques sont numérisés et stockés dans COSMOS ou IRIS.

Responsabilités ministérielles et interconnectivité des systèmes

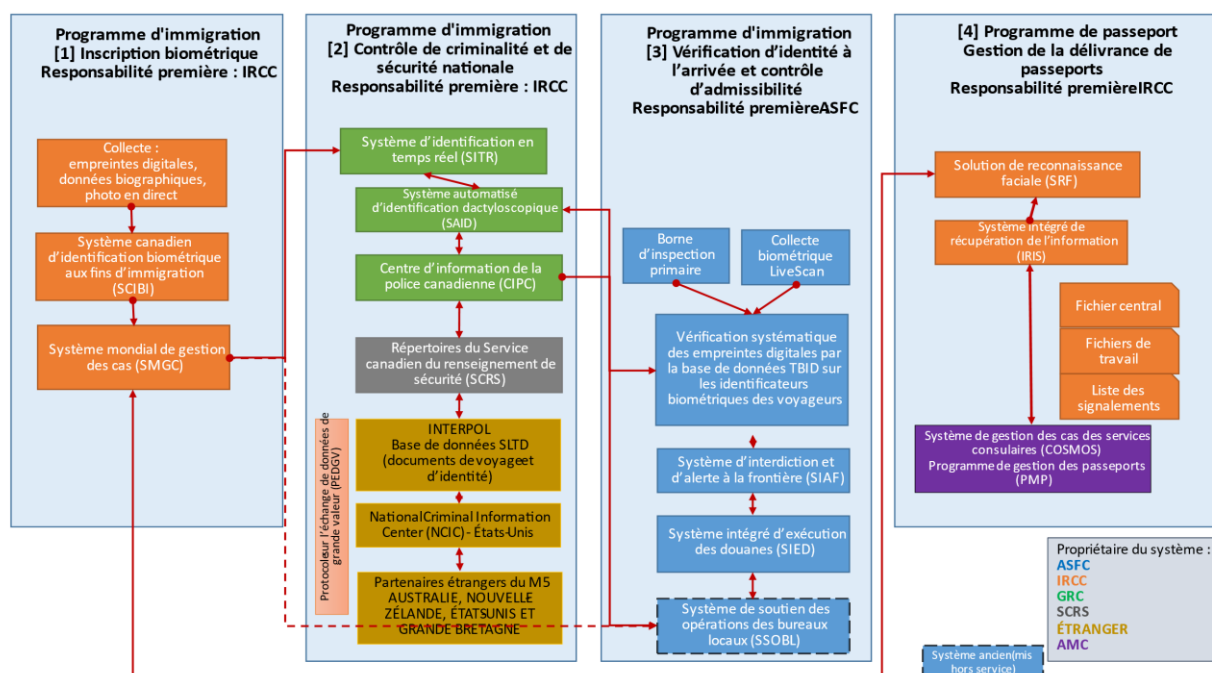


Figure 2 : Responsabilités ministérielles et interconnectivité des systèmes

[1] Inscription biométrique (IRCC)

IRCC est le ministère principalement responsable de la collecte et de la gestion des données biométriques aux fins du Programme d'immigration. La collecte des données biométriques et des renseignements biographiques connexes (empreintes digitales, données biographiques, photographies en direct) se fait dans un lieu d'inscription et est suivie de leur transmission sécuritaire au SCIBI à IRCC. Au reçu par le SCIBI des données biométriques et des données biographiques liées, les empreintes digitales sont communiquées en toute sécurité au SITR de la GRC. Après une recherche automatique par la GRC, les résultats reviennent à IRCC dans le dossier de cas du SMGC. Les données biographiques et les photographies en direct du SCIBI sont versées aux dossiers de cas du SMGC. Une fois les vérifications faites, un agent des visas prend la décision définitive et, si un visa de résident temporaire est approuvé, un avis est envoyé à l'ASFC pour un ajout aux dossiers opérationnels.

[2] Contrôle de criminalité et de sécurité nationale (IRCC)

Une fois le demandeur inscrit, des vérifications sont effectuées pour éclairer les décisions en matière d'admissibilité. Ces vérifications consistent en plusieurs recherches fondées sur les empreintes digitales et les données biographiques. Elles s'amorcent quand le SMGC envoie des messages en vérification d'empreintes au SITR qui, par le SAID, procédera à une identification dactyloscopique automatique. Cette étape se fait en interface avec d'autres systèmes comme le CIPC, les répertoires du SCRS et les répertoires étrangers. Si des indicateurs sont rouges, il y a renvoi au SMGC en vue d'un examen par un agent d'immigration. S'il n'y a pas de résultat défavorable, le SMGC en prend note et les données du demandeur sont envoyées au SSOBL de l'ASFC pour être enregistrées en prévision de l'arrivée du demandeur au Canada.

[3] Vérification d'identité à l'arrivée et contrôle d'admissibilité (ASFC)

Lorsque le demandeur arrive à un point d'entrée et se présente à une borne d'inspection primaire ou à un terminal LiveScan, une vérification systématique des empreintes digitales vient confirmer l'identité de l'intéressé par une recherche dans les systèmes du TBID et du SAID. L'ASFC exerce un contrôle supplémentaire par le SIAF, le SIED et le SSOBL. D'ailleurs, si un résident temporaire devient connu des organismes d'application de la loi, toute inscription d'empreintes digitales dans le CIPC produira un indicateur qui parviendra au SSOBL de l'ASFC. Le SSOBL le relatera alors au SMGC d'IRCC pour une correspondance dans les fonds de renseignements des résidents temporaires.

[4] Gestion de la délivrance des passeports (IRCC)

Les demandes de passeports et de documents de voyage au Canada sont gérées dans le système IRIS ou SMGC qui passera par le système SRF pour comparer un modèle biométrique facial aux dossiers existants afin de vérifier l'identité du demandeur et de prévenir la fraude. Si le demandeur est à l'étranger, le système COSMOS est utilisé pour traiter sa demande et s'interface avec IRIS, le dossier étant finalement stocké dans le fichier central.