PUBLICATION CONCERNANT LE RÉSEAU CANADIEN D'INFORMATION POUR LA SÉCURITÉ PUBLIQUE

IIJ@l'ŒUVRE

ÉTÉ 2004, VOLUME 3, NUMÉRO 1

COMBATTRE LE TERRORISME À L'AIDE DE LA BIOMÉTRIE

L'interopérabilité : LA PROCHAINE ÉTAPE DE L'ÉVOLUTION DE L'IIJ AU CANADA

PROFIL DE PARTENAIRES : LE QUÉBEC ET LA SASKATCHEWAN SE BRANCHENT AU SGD

LE PORTAIL D'INFORMATION POLICIÈRE ENTRE EN SERVICE EN COLOMBIE-BRITANNIQUE ET EN ONTARIO

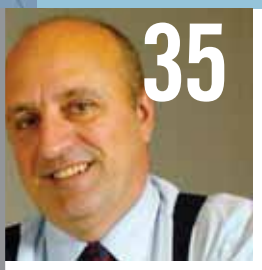
Canada

TABLE DES MATIÈRES

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE

PROFIL DE L'INTEROPÉRABILITÉ

PROFILS DE PARTENAIRES



À PROPOS D'*IIJ@L'ŒUVRE*

IIJ@l'œuvre *est publiée par le Secrétariat de l'intégration de l'information de la justice, du ministère de la Sécurité publique et de la Protection civile du Canada. Les opinions et les points de vue exprimés dans cette publication ne reflètent pas nécessairement ceux du Ministère.*

ISSN 1703-0129
Volume 3, numéro 1

Imprimé au Canada

DIRECTEUR EXÉCUTIF *Greg Wright*
RÉDACTRICE EN CHEF *Eleanor Willing*
COLLABORATEURS *Patrick Gant, thinkit communications*
Andrew Kirkwood, Stiff Sentences Inc.
CONCEPTION GRAPHIQUE *Accurate Design and Communication Inc.*
PHOTOGRAPHIE *tecklesphoto.com*

*L'équipe d'*IIJ@l'œuvre *serait heureuse de publier vos articles et lettres d'opinion, ainsi que de connaître vos suggestions d'articles.*

Les textes soumis sont susceptibles d'être révisés sur le plan du style et de la longueur. Tous les collaborateurs doivent indiquer leur adresse de courrier électronique et le numéro de téléphone où on peut les joindre pendant la journée.

Faites parvenir vos envois à l'adresse suivante :
IIJ@l'œuvre
Sécurité publique et Protection civile Canada
Secrétariat de l'intégration de l'information de la justice
340, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Téléphone : (613) 991-4279
Télécopieur : (613) 991-3306
Site Web : www.sppcc-psepc.gc.ca
Courriel : ijis-siij@psepc-sppcc.gc.ca

AVANT-PROPOS

Un message de l'honorable Anne McLellan, vice-première ministre et ministre de la Sécurité publique et de la Protection civile du Canada

À titre de vice-première ministre et ministre de la Sécurité publique et de la Protection civile du Canada, je suis heureuse d'avoir l'occasion de saluer les lecteurs et lectrices d'*IIJ@l'œuvre*.

Le 12 décembre 2003, le premier ministre a annoncé la création d'un nouveau ministère, Sécurité publique et Protection civile Canada (SPPCC). Ce ministère regroupe les fonctions centrales de la sécurité et du renseignement, des services de police et d'application de la loi, des services correctionnels et de la prévention du crime, des services frontaliers et de l'intégrité des frontières, de l'application de la législation en matière d'immigration et de la gestion des mesures d'urgence.

La création de SPPCC et de ses organismes est un élément clé des efforts que déploie le gouvernement du Canada pour mieux assurer la sécurité publique au Canada. En collaboration avec ses partenaires de tous les paliers de gouvernement et de tous les secteurs de la société, SPPCC s'efforce de bâtir un Canada plus sécuritaire et plus sûr qui respecte les libertés fondamentales d'une démocratie pluraliste tout en répondant aux attentes des citoyens et citoyennes en matière de sécurité collective.

Ces partenaires nous sont indispensables et doivent par conséquent évoluer dans un environnement qui favorise l'échange de renseignements et d'idées. Grâce à la présente publication, *IIJ@l'œuvre*, le Secrétariat de l'intégration de l'information de la justice continue de jouer ce rôle important d'appui à la sécurité publique.

La population en général, les intervenants et intervenantes intéressés, les partenaires du Réseau canadien de l'information pour la sécurité publique (RCISP) de même que le personnel de première ligne de la justice pénale et de la sécurité publique peuvent être fiers des réalisations du Canada, à ce jour, en matière d'intégration de l'information de la justice — bon nombre de celles-ci sont d'ailleurs décrites dans la présente publication. Chaque réalisation est un pas en avant pour la sécurité publique et la justice pénale au Canada et à l'étranger.

Je vous invite à continuer de collaborer avec vos partenaires nationaux et internationaux afin de préserver et d'améliorer la sécurité des Canadiens et Canadiennes.

L'honorable A. Anne McLellan, C.P., députée
vice-première ministre et ministre de la
Sécurité publique et de la Protection civile
du Canada

NOTE DE LA RÉDACTRICE EN CHEF

Le changement est une force constamment à l'œuvre dans la nature, et les partenaires de la collectivité de l'intégration de l'information de la justice ne sont pas immunisés contre ce phénomène. Entre ce quatrième numéro d'*IIJ@l'œuvre* et le numéro antérieur, le portefeuille de la sécurité publique du gouvernement du Canada a subi de très importants changements, notamment la création de notre nouveau ministère, Sécurité publique et Protection civile Canada, et le lancement de la toute première politique canadienne intégrée de sécurité nationale.

Ces changements s'inscrivent dans le cadre de transformations beaucoup plus profondes qui sont en cours au sein des collectivités chargées de la gestion de la sécurité publique et de la justice pénale au Canada. L'interopérabilité et la biométrie, utilisées dans différents projets gouvernementaux, ouvrent de formidables possibilités d'échanger des renseignements dans un environnement contrôlé et sécurisé.

C'est parce que nous reconnaissons l'importance de ces changements que nous avons consacré une grande partie de la présente publication à mettre en évidence les efforts déployés actuellement partout au Canada. Chaque article montre comment des percées importantes peuvent faire progresser notre objectif commun, celui de l'intégration de l'information de la justice.

Le Réseau canadien d'information pour la sécurité publique tire une bonne partie de sa force des réalisations de ses partenaires, toujours à la recherche de meilleures méthodes de travail collectif et d'échange de renseignements. C'est la raison pour laquelle le présent numéro d'*IIJ@l'œuvre* met également en lumière les principales réalisations des provinces, y compris une entente entre le Service correctionnel du Canada et le Québec, la Saskatchewan et la Colombie-Britannique; des efforts de collaboration au chapitre du maintien de l'ordre en Ontario et en Colombie-Britannique; ainsi que les points saillants de récentes conférences sur la mise en commun de l'information, la technologie et la lutte contre le terrorisme.

Comme toujours, je suis intéressée à savoir ce que vous pensez d'*IIJ@l'œuvre*. Vous pouvez nous faire part de vos impressions par courriel à l'adresse suivante : ijis-siij@sppcc-psepc.gc.ca. Vos commentaires influenceront sans doute le contenu des prochains numéros de la revue.

Eleanor Willing

Eleanor Willing
Rédactrice en chef, *IIJ@l'œuvre*

L'INTEROPÉRABILITÉ AU CANADA :

Préparer la prochaine étape de l'évolution de l'intégration de l'information de la justice au Canada

L'interopérabilité est un terme qui fait de plus en plus partie du vocabulaire des collectivités œuvrant dans les secteurs de la sécurité publique, de la justice pénale et de la technologie de l'information. Et l'intérêt pour ce terme et ses nombreuses applications ne se limite pas au Canada. Une recherche par mot clé à l'aide de Google (un populaire moteur de recherche sur Internet) génère plus de deux millions d'occurrences accompagnées de liens à des organisations de justice pénale, de technologie et de sécurité partout dans le monde. Mais une définition type de l'interopérabilité — la capacité de communication entre des unités fonctionnelles différentes utilisant des logiciels et des appareils provenant de multiples fournisseurs — ne donne qu'une faible idée du potentiel réel de l'interopérabilité et des difficultés à surmonter pour la rendre possible.

Aucun pays n'a encore atteint la pleine interopérabilité ou la mise en commun parfaite de l'information, mais cette situation pourrait changer rapidement. Les efforts déployés par les partenaires du Réseau canadien d'information pour la sécurité publique (RCISP) ont ouvert la voie à l'amélioration de l'interopérabilité parmi les organisations canadiennes oeuvrant dans les secteurs de la justice pénale et de la sécurité publique — préparant ainsi la prochaine étape de l'évolution de l'intégration de l'information de la justice dans ce pays.

Grâce au Réseau canadien d'information pour la sécurité publique, tout est en place pour améliorer l'interopérabilité entre les organismes de la justice pénale et de la sécurité publique.

En 2005, le RCISP aura atteint les principaux objectifs de son plan d'action quinquennal. Il lui sera donc beaucoup plus facile de mettre de l'avant des initiatives d'intégration de l'information de la justice — et bien sûr d'interopérabilité dans l'ensemble du secteur de la sécurité publique.

CE QUE SIGNIFIE L'INTEROPÉRABILITÉ POUR LES CITOYENS ET CITOYENNES

Les Canadiens et Canadiennes pourront bientôt observer par eux-mêmes les résultats de l'interopérabilité dans les rues, dans les aéroports, dans les tribunaux et dans de nombreux autres endroits publics. À titre d'exemple, les services policiers pourront échanger facilement de l'information sur la justice pénale avec leurs homologues des services correctionnels et de libération conditionnelle, en utilisant des normes communes de données et en souscrivant à un dictionnaire unique des termes, descriptions et infractions concernant des affaires de justice pénale. Par la suite, les tribunaux pourront avoir accès aux renseignements réunis par les organisations

PROFIL DE L'INTEROPÉRABILITÉ

correctionnelles et les commissions de libération conditionnelle, toujours grâce à l'adoption de normes communes de données et d'un dictionnaire commun de l'information. Déjà, les douanes peuvent relever un numéro de plaque d'immatriculation sur un véhicule à un poste frontalier, et savoir sur-le-champ s'il s'agit d'un véhicule recherché par la police. Les applications possibles de l'interopérabilité dans le secteur de la sécurité sont sans fin, et ses ramifications pourront sans doute améliorer la sécurité de tous les Canadiens et Canadiennes.

L'interopérabilité et les nouvelles possibilités de mise en commun de l'information ne deviendront pas réalité du jour au lendemain. Il faudra du temps pour cela. Il reste encore du travail à faire pour rendre l'environnement entièrement interfonctionnel et parvenir à coordonner la circulation de l'information au sein de la collectivité chargée de la sécurité publique. L'une des initiatives actuellement à l'étude dans ce domaine permettra à des partenaires d'échanger des renseignements secrets dans un réseau sécurisé.

UN NOUVEAU PROJET SOUTENU PAR UN NOUVEAU MINISTÈRE

Le Secrétariat de l'IIJ a reçu avec enthousiasme l'annonce du nouveau projet sur l'interopérabilité, lancé en mai 2004. Au cours des 18 prochains mois, le projet sur l'interopérabilité a pour objectif d'élaborer une vision globale et un plan stratégique permettant de créer un environnement d'interopérabilité durable, qui servira les intérêts du gouvernement du Canada en matière de sécurité publique. Sur les plans juridique et stratégique, ce projet a des défis particuliers à relever, notamment celui de faire respecter les droits de chaque personne à la protection des renseignements personnels la concernant.

La nécessité de faire participer les principaux organismes au projet sur l'interopérabilité découle en partie de la création du nouveau ministère de la Sécurité publique et de la Protection civile du Canada (SPPCC).

Ce ministère dirigera le travail sur l'interopérabilité et veillera à consulter et informer les autres intervenants en matière de sécurité publique. L'équipe responsable du projet sur l'interopérabilité axe déjà ses efforts sur une première étape clé — la rédaction d'un rapport provisoire qui sera présenté au Cabinet fédéral à l'automne de 2004 et dans lequel seront définies les priorités les plus pressantes.

TROUVER UNE SOLUTION ABORDABLE

Carrie Hunter (directrice de la Division de l'interopérabilité) aime bien attirer l'attention sur la pensée affichée sur son babillard : « Si nous n'avons pas les moyens d'appliquer la solution, ce n'est pas une solution ». Telle est l'essence du défi à relever, explique-t-elle. « Cette phrase rappelle, non seulement à nos fournisseurs,

Carrie Hunter, directrice de la Division de l'interopérabilité, Secrétariat de l'intégration de l'information de la justice (SIIJ)

« Si nous n'avons pas les moyens de réaliser la solution, ce n'est pas une solution. »

AMÉLIORER LA SÉCURITÉ PUBLIQUE AU CANADA

Afin d'assurer la sécurité publique, le gouvernement a adopté les mesures suivantes :

- création du nouveau ministère de la Sécurité publique et de la Protection civile, qui permet d'améliorer la coordination et de regrouper certains services essentiels et certaines responsabilités dans un même ministère fédéral;
- annonce de la mise sur pied d'un projet sur l'échange d'information en matière de sécurité publique et l'interopérabilité, qui vise à combler les lacunes concernant l'interopérabilité et à assurer des communications efficaces et sécurisées entre toutes les organisations qui assument des responsabilités importantes dans le secteur de la sécurité publique;
- création de l'Agence des services frontaliers du Canada, qui réunit plusieurs fonctions clés auparavant réparties entre trois organismes — le programme des douanes de l'Agence des douanes et du revenu du Canada; le programme du renseignement, des interceptions et de l'exécution de Citoyenneté et Immigration Canada; ainsi que le programme d'inspection des importations dans les bureaux d'entrée de l'Agence canadienne d'inspection des aliments;
- lancement de la toute première Politique intégrée de sécurité nationale du Canada, qui permet de coordonner les efforts de partenaires de l'intérieur du pays et de l'étranger afin de contrer la menace qui plane sur la sécurité nationale canadienne.

« Jusqu'à maintenant, les solutions proposées étaient généralement des solutions à la pièce, mises en œuvre de manière ponctuelle, ministère par ministère. Nous n'avons pas de solution globale qui pourrait convenir à l'ensemble du gouvernement du Canada. »

mais aussi à ceux d'entre nous, au gouvernement, qui travaillent sur l'interopérabilité et sur les autres activités liées à l'intégration de l'information de la justice, que nous devons agir de manière pratique. »

À titre de directrice de la Division de l'interopérabilité au Secrétariat de l'intégration de l'information de la justice, Mme Hunter veut s'assurer que l'interopérabilité ne deviendra pas un projet de technologie de l'information aussi coûteux que prometteur. Loin de là : « Nous voulons trouver le moyen d'atteindre nos objectifs de la façon la plus facile et la plus efficace possible pour les citoyens et citoyennes », dit-elle.

Mais dans ce nouveau projet, la recherche d'une solution peu coûteuse n'est que le début du travail. « Nous voulons aussi susciter des changements importants dans les pratiques de gestion de l'information et de technologie de l'information (GI/TI) au sein du gouvernement du Canada », explique-t-elle. « Ce faisant, nous nous efforçons de créer un nouvel environnement dans lequel l'interopérabilité peut influencer la façon dont nous achetons et la nature de nos achats en ce qui concerne les nouvelles technologies. »

LA NON-INTEROPÉRABILITÉ

Mme Hunter affirme toutefois que ce projet aura des répercussions sur la collectivité responsable de la sécurité publique à l'intérieur et à l'extérieur du gouvernement. Au gouvernement, il y a beaucoup trop de systèmes de technologie de l'information qui sont dans un état de non-interopérabilité — processus et structures monolithiques incapables d'atteindre un niveau important d'échange de renseignements avec les systèmes des autres ministères ou paliers de gouvernement. « Nous devons être en mesure d'autoriser ou de bloquer facilement les flux de l'information lorsque les circonstances et la loi l'exigent », dit-elle; « c'est là un aspect important, car nous sommes constamment confrontés à de nouveaux défis en matière de sécurité publique. »

De multiples raisons expliquent pourquoi la non-interopérabilité est si fréquente dans l'ensemble du gouvernement — l'âge, la conception et les fonctions désuètes de nombreux systèmes de GI/TI, par exemple — mais il existe également des motifs opérationnels.

Mme Hunter estime que les pratiques inhérentes à la passation des marchés au gouvernement fédéral et la compétitivité entre les fournisseurs sont des obstacles majeurs à l'interopérabilité. « Nous avons découvert que l'interopérabilité ne figurait pas parmi les principaux critères d'évaluation utilisés par Travaux publics et Services gouvernementaux Canada pour déterminer le soumissionnaire gagnant lors de l'attribution d'un contrat », dit-elle. « Nous aimerions que cela change. »

En ce qui concerne les fournisseurs, Mme Hunter fait remarquer que « certains ont tendance, probablement pour des motifs de compétitivité, à créer des systèmes fermés afin que la clientèle reste fidèle à leurs produits. » Les utilisateurs sont confrontés quotidiennement aux effets de cette pratique : allant de bases de données qui ne peuvent s'échanger des données à des documents qui ne peuvent être ouverts sur les systèmes informatiques des bureaux qui emploient des logiciels différents. Il en découle que la recherche de solutions de rechange fait perdre du temps — ou pire encore — que certains partenaires ne peuvent tout simplement pas échanger de renseignements.

L'interopérabilité n'est pas une solution qui consiste à acheter du nouveau matériel ou de nouveaux logiciels. Elle ne peut devenir réalité qu'en modifiant bon nombre des pratiques qui caractérisent le déroulement des opérations dans les ministères fédéraux, y compris le mode d'acquisition du matériel et de la technologie.

C'est pour tenter de résoudre ce genre de problèmes que la Division de l'interopérabilité invite les fournisseurs de technologie de l'information à se joindre à un groupe de travail bénévole qui a pour mandat d'étudier des façons d'assurer l'interopérabilité intrinsèque de leurs produits. Mme Hunter est encouragée par la réaction des fournisseurs à son invitation, et s'attend à ce que le groupe de travail tienne sa première réunion au plus tard au milieu de l'année 2004.

PROFIL DE L'INTEROPÉRABILITÉ

FINI LES SOLUTIONS À LA PIÈCE

Comme l'explique M^me^ Hunter, les tentatives faites à ce jour pour résoudre la question de l'interopérabilité ont également créé des problèmes. « Jusqu'à maintenant, les solutions proposées étaient généralement des solutions à la pièce, mises en œuvre de manière ponctuelle, ministère par ministère. Nous n'avons pas de solution globale qui pourrait convenir à l'ensemble du gouvernement du Canada. » Le nouveau projet sur l'interopérabilité, dirigé par Mark Bornais (directeur de projet), aidera à corriger cette situation — non seulement grâce au vaste mandat du ministère responsable, mais aussi parce que la portée des travaux va au-delà du système de justice pénale pour englober d'autres organismes de sécurité publique.

Et M^me^ Hunter d'ajouter : « Nous sommes tout à fait disposés à collaborer avec d'autres organismes — de sécurité publique ou de sécurité nationale — afin de les aider à découvrir ce qui les empêche d'atteindre la pleine interopérabilité avec leurs partenaires ».

ÉTABLIR LE BIEN-FONDÉ D'UNE APPROCHE COMMUNE

Afin d'illustrer la nécessité d'une approche commune de l'interopérabilité au sein du gouvernement fédéral, M^me^ Hunter cite une étude de cas. Au cours de l'exercice 2002-2003, l'ancienne Agence des douanes et du revenu du Canada travaillait avec ses homologues des États-Unis à l'élaboration d'un système d'échange de renseignements visant à fournir aux autorités de l'information préalable sur les voyageurs de tous les vols à destination des États-Unis. Le rôle du Canada consistait à concevoir un système permettant de recueillir des renseignements auprès des compagnies aériennes et de procéder à un contrôle de sécurité des passagers avant leur arrivée. Entre-temps, la GRC, le SCRS et Transports Canada envisageaient une initiative semblable en vertu de la *Loi sur la sécurité publique*. Dans ce dernier cas, les renseignements recueillis devaient servir à repérer les criminels et les présumés terroristes qui pourraient tenter de monter à bord d'un avion.

Le chevauchement des deux systèmes de GI/TI proposés était frappant — tous les champs de données, sauf trois, étaient identiques. « Différents secteurs de nos organisations avaient participé à la conception de ces systèmes », explique M^me^ Hunter. « Heureusement, les personnes concernées se sont parlé et sont parvenues à s'entendre sur une manière efficace d'atteindre les deux objectifs. » Elle ajoute qu'on peut éviter les possibilités de chevauchement ou de dépassement « en assurant la coordination de tous les projets de technologie de l'information qui touchent la communication de renseignements et l'interopérabilité, et en veillant à ce que les liens entre les différents projets soient bien compris ».

Force est de reconnaître qu'il faudra encore du temps pour que l'interopérabilité devienne réalité au sein du nouveau ministère. Les travaux du projet sur l'interopérabilité viennent tout juste de débuter — ils ressemblent davantage à une mission de dépistage et de recherche ayant pour but d'énoncer clairement les choix qui s'offrent au gouvernement du Canada. Et M^me^ Hunter de conclure : « Nous ne pouvons présumer du résultat de cette démarche, mais nous avons la certitude que l'interopérabilité orientera l'évolution du Réseau canadien d'information pour la sécurité publique au cours des prochaines années et même de la prochaine décennie ».

« Le projet sur l'interopérabilité ressemble à une mission de dépistage et de recherche ayant pour but d'énoncer clairement les choix qui s'offrent au gouvernement du Canada. »

PROFIL DE L'INTEROPÉRABILITÉ

ME RECEVEZ-VOUS?

LES DÉFIS PARTICULIERS DE L'INTEROPÉRABILITÉ RADIO

On fait souvent observer que les activités criminelles, les catastrophes naturelles et les actes terroristes ne tiennent aucun compte des limites territoriales. Et c'est la raison pour laquelle les organismes de sécurité publique doivent absolument établir des communications transfrontières immédiates et continues.

À la GRC, André Laflèche et Francine Boucher font partie d'une équipe chargée de rendre ce genre de communications possible grâce à l'*interopérabilité radio*, laquelle met à la disposition des organismes d'application de la loi et d'autres organismes les outils dont ils ont besoin pour communiquer en temps réel sans se soucier des frontières, tant opérationnelles que géographiques.

Tour de télécommunications à Kelowna (C.-B.) partagée par la GRC, NAV Canada et Telus.

Photo reproduite avec l'aimable autorisation de Dave Patterson, GRC

PROFIL DE L'INTEROPÉRABILITÉ

Dans le cadre d'un projet pilote en voie de réalisation dans la région de Windsor, en Ontario, M. Laflèche et M^me^ Boucher ainsi que leurs collègues sont parvenus à une vision commune, claire et à long terme, de ce qu'exige réellement l'interopérabilité.

UN DÉFI À MULTIPLES ASPECTS

L'existence de limites de compétence à différents paliers complique la mise en œuvre de l'interopérabilité radio. De nombreux organismes peuvent être actifs dans une seule région métropolitaine — leurs « compétences » étant définies par leur rôle et leur mandat. Leurs activités peuvent se dérouler aux extrémités opposées du territoire de la ville, le long des frontières provinciales et même le long de la frontière internationale entre le Canada et les États-Unis.

En fait, c'est ce dernier cas qui a d'abord incité la GRC à mettre sur pied une équipe chargée d'étudier l'interopérabilité radio. À la réunion de l'été 2002 du Forum sur la criminalité transfrontalière Canada-États-Unis, il a été convenu que les organismes à l'œuvre de chaque côté de la frontière devaient avoir la possibilité, dans l'intérêt de la sécurité publique, de se transmettre de l'information opérationnelle.

André Laflèche — gestionnaire principal du projet sur les systèmes, aux Services de communications mobiles de la GRC — a reçu le mandat de proposer des solutions provisoires et d'élaborer une stratégie à long terme d'interopérabilité.

« Dans une ville comme Ottawa », explique M. Laflèche, « il est relativement simple pour les organismes locaux — par exemple, la GRC et la Police d'Ottawa — de se rencontrer et d'élaborer un accord d'échange de renseignements. La première assume des responsabilités fédérales et la seconde des responsabilités municipales, mais les deux organismes interviennent à peu près au même palier et couvrent sensiblement le même territoire. Et c'est exactement ce qu'ils ont fait en concluant un accord « Police de protection — Services généraux », qui leur permet de s'entraider. Mais lorsqu'il s'agit de la frontière canado-américaine, les choses se compliquent parce que nous parlons alors d'accords internationaux, qui sont nécessairement plus complexes — et que les organismes ne sont pas autorisés à négocier de leur propre chef.

M. Laflèche affirme que lui-même et son équipe croyaient au départ que de tels accords devaient être de nature opérationnelle, mais que cela s'est révélé trop compliqué dans la pratique. « Tous ces organismes — la police, les douanes, la patrouille frontalière — ont des mandats et des méthodes de travail qui leur sont propres », dit-il. « Tenter de définir ces mandats et méthodes de manière détaillée ou de les *redéfinir*, dans le contexte de l'interopérabilité, est une tâche trop colossale. »

M. Laflèche a plutôt décidé qu'il valait mieux axer les efforts sur les questions de communication : qui doit parler à qui et dans quelles circonstances? « Bien sûr, vous devez être au courant de ce qui se passe dans la pratique », s'empresse-t-il d'ajouter. « Il faut toujours se reporter aux exigences du service. »

LA QUESTION DE LA TECHNOLOGIE

M. Laflèche fait observer que la technique est maintenant suffisamment perfectionnée pour rendre les communications très efficaces entre différents réseaux radio. Mais il ajoute que ce qui est bon pour aujourd'hui ne le sera pas nécessairement pour demain.

« Nous sommes entre deux paradigmes », dit-il, « l'analogique et le numérique. Les nouvelles technologies, les technologies numériques, nous donnent beaucoup de liberté et nous permettent de diviser et subdiviser une fréquence donnée en canaux contrôlés. Nous gagnons donc en flexibilité et en fonctionnalité. Mais par ailleurs, les technologies numériques sont beaucoup plus complexes que les technologies analogiques, ce qui —ajouté à leur manque de normalisation — les rend plus difficiles à intégrer. »

Comme il fallait s'y attendre, M. Laflèche est convaincu que les solutions numériques prédomineront à long terme — surtout parce ce qu'elles permettent à la fois la communication vocale et la communication de données. « Mais pour l'instant », dit-il, « les organismes veulent, tout naturellement, prolonger le plus possible la durée de vie des systèmes existants. Différentes technologies sont donc utilisées en même temps. Pour obtenir une interopérabilité à court terme, nous devons opter pour une approche tactique et pragmatique ». C'est exactement le genre d'approche que M. Laflèche et son équipe ont retenu pour leur projet de Windsor. Mais avant de décrire ces travaux plus en détail, il faut parler d'un autre facteur dont l'interopérabilité radio doit tenir compte : la gestion du spectre.

QU'EST-CE QUE LA FRÉQUENCE?

Une collègue de M. Laflèche, Francine Boucher, est ingénieure principale des systèmes et gestionnaire de la section responsable de la gestion du spectre des radiofréquences aux Services de communications mobiles de la GRC. Elle fait observer qu'au Canada et aux États-Unis le spectre des radiofréquences est presque entièrement attribué.

« Les nouvelles technologies et les technologies numériques nous donnent beaucoup de liberté et nous permettent de diviser et de subdiviser une fréquence donnée en canaux contrôlés.iviser une fréquence donnée en canaux contrôlés. »

PROFIL DE L'INTEROPÉRABILITÉ

« Il n'est pas facile pour les organismes responsables de la délivrance de licences d'utilisation du spectre d'ouvrir de nouvelles bandes », dit-elle. Au Canada, cet organisme est Industrie Canada; aux États-Unis, la responsabilité est partagée entre la National Telecommunications and Information Administration (NTIA) et la U.S. Federal Communications Commission (FCC). « Ces organismes doivent présenter une demande à l'Union internationale des télécommunications (UIT), laquelle ne convoque la Conférence mondiale des radiocommunications qu'une fois tous les trois ans. Ils doivent donc être très vigilants et se montrer réfléchis dans leur façon d'attribuer les parties du spectre qui sont disponibles. »

Cette situation risque de compliquer encore davantage la négociation des accords transfrontaliers de communications.

« Lorsqu'un service de police canadien veut ouvrir sa radiofréquence à un homologue américain », explique M^me^ Boucher, « il est possible que quelqu'un possède déjà une licence pour cette même fréquence, à d'autres fins, de l'autre côté de la frontière, et vice versa. Comment résoudre ce problème? »

Phuong Vu est gestionnaire du génie du spectre pour les services de communications mobiles et personnelles à Industrie Canada. Il affirme que son ministère est fermement résolu à surmonter ce genre d'obstacles et travaille actuellement avec la NTIA et la FCC à simplifier le processus d'autorisation pour l'attribution des bandes de fréquence le long de la frontière. « Nous avons tenté de cerner les problèmes, en 2002, lors d'une conférence nationale sur les radiocommunications et la sécurité publique », dit M. Vu. « Nous sommes très intéressés à améliorer l'interopérabilité radio, et nous sommes conscients du fait que le spectre fait partie de l'équation. »

Cela dit, il estime que le plus important, à ce stade-ci, est d'élaborer une sorte de plan national — une stratégie pour l'interopérabilité radio dont Industrie Canada pourrait se servir pour établir les priorités concrètes de la gestion du spectre à l'avenir.

« Le plus important, à ce stade-ci, c'est d'élaborer une sorte de plan national — une stratégie pour l'interopérabilité radio dont Industrie Canada pourrait se servir pour établir des priorités concrètes. »

Les assises d'une telle stratégie sont en train d'être posées en ce moment même à Windsor.

ÉTUDE DE CAS PRATIQUE

À bien des égards, Windsor est un endroit idéal pour étudier l'interopérabilité radio à l'œuvre. Située sur une péninsule du sud-ouest de l'Ontario — à la frontière des États-Unis — cette ville constitue un milieu relativement fermé dans lequel évoluent des organismes tels que la police de Windsor, la Police provinciale de l'Ontario, l'Agence des services frontaliers du Canada, la patrouille frontalière américaine et les douanes américaines.

C'est la raison pour laquelle une équipe intégrée de la police des frontières (EIPF) est déjà en poste dans la région de Windsor. (La première équipe de ce genre a vu le jour en 1996; elle était composée de représentants d'organismes d'application de la loi de la Colombie-Britannique et de l'État de Washington.)

Pour étudier l'interopérabilité radio, la GRC mise actuellement sur les partenariats déjà établis dans le cadre du programme qui a permis la création de l'EIPF à Windsor.

André Laflèche explique que « les solutions provisoires proposées à ce jour consistent à mettre en service des appareils qui permettent une interopérabilité tactique. Les organismes se choisissent des partenaires pour des opérations préalablement définies et utilisent nos appareils comme passerelles entre leurs réseaux de communications ». Pour le moment, il s'agit d'un processus plutôt lourd, à forte intensité de main-d'œuvre, qui exige que les connexions soient établies une par une. Mais ce qui intéresse le plus M. Laflèche, ce n'est pas la méthode de connectivité, mais la façon dont la connectivité est utilisée.

« Le projet de Windsor nous permet d'observer ce que les organismes font avec ces outils de communications — quelles sont leurs priorités. Les résultats de ce projet orienteront notre stratégie à long terme d'interopérabilité. »

L'approche a été élaborée en collaboration avec des membres d'expérience du personnel opérationnel et technique de la GRC.

PROCHAINES ÉTAPES

Alors même que l'interopérabilité fait l'objet d'études sur le terrain, des questions d'ordre stratégique sont abordées ailleurs. Ainsi, un projet d'accord d'échange de renseignements a été élaboré par la GRC et examiné par l'équipe intégrée de la police des frontières de Windsor, ainsi que par les douanes et la patrouille frontalière américaines, et il fait actuellement l'objet d'un examen juridique.

En ce qui concerne l'avenir, André Laflèche et Francine Boucher croient tous les deux qu'après qu'on aura élaboré une stratégie à long terme, le moment sera peut-être venu de désigner un ministère directeur et de préciser le mandat de la gouvernance de l'interopérabilité radio à titre d'activité nationale.

« Nous sommes persuadés qu'il existe une réelle volonté d'atteindre ces objectifs », dit M. Laflèche. « Je pense que le travail que nous faisons maintenant pour tenter de définir les besoins favorisera l'alignement des priorités des différents organismes et nous indiquera la direction à suivre à l'avenir. »

SUR UN PLATEAU D'ARGENT

L'OUTIL DE RECHERCHE INTÉGRÉ DE LA GRC – UNE SEULE INTERFACE POUR ACCÉDER À PLUSIEURS DÉPÔTS CENTRAUX DE RENSEIGNEMENTS

Photo reproduite avec l'aimable autorisation de la GRC

En novembre 2001, la GRC a entrepris de concevoir un nouveau système électronique de gestion des cas et des dossiers, doté d'une grande fonctionnalité pratique et adapté aux besoins réels des utilisateurs de première ligne. Ce système, c'était le SIRP : le Système d'incidents et de rapports de police.

Le SIRP devait remplacer le système de gestion des dossiers utilisé actuellement par la GRC, le SRRJ (Système de récupération de renseignements judiciaires). Dès le départ, on savait que le processus de remplacement devait être graduel. Le SRRJ contenait trop de renseignements précieux pour qu'on le mette tout simplement hors d'usage, et (pour des raisons pratiques) la migration de son contenu vers le nouveau système avait été reportée de cinq ans.

Devant la perspective du maintien de systèmes parallèles — tous les deux reliés à la base de données du Centre d'information de la police canadienne (CIPC) — la GRC a décidé qu'elle avait surtout besoin d'un outil permettant d'effectuer la jonction avec les trois sources d'information. Et c'est ainsi que l'Outil de recherche intégré (ORI) a vu le jour.

UNE FENÊTRE, TROIS VUES

Comme son nom l'indique, l'ORI fournit un mécanisme unique pour interroger le contenu du SIRP, du SRRJ et de la base de données principale du CIPC — en présentant dans un format normalisé les résultats en provenance des trois sources. Il en est aux dernières étapes de son élaboration et il devrait être mis en œuvre au moment du lancement officiel du SIRP, à l'été 2004.

PROFIL DE L'INTEROPÉRABILITÉ

Les utilisateurs qui se connectent à l'ORI — un outil entièrement sécurisé à l'aide d'une infrastructure à clé publique (ICP) Entrust — ont différentes options de recherche : d'une personne, d'une entreprise ou organisation, d'un bien, d'un identificateur (ID) unique et d'un véhicule. Les recherches dans l'une ou l'autre de ces catégories permettent d'obtenir une liste des résultats établie en fonction des privilèges de l'autorisation de l'utilisateur à l'égard des systèmes sources. Les membres ont alors la possibilité de visualiser des détails supplémentaires et les dossiers d'incidents connexes à partir de la liste des résultats.

Une autre caractéristique de l'ORI est sa capacité d'accéder directement aux applications SRRJ et SIRP par l'intermédiaire d'un mécanisme unique et commode d'entrée en communication. Bien entendu, les membres doivent d'abord avoir installé le logiciel d'application du SIRP sur leurs postes de travail — et avoir obtenu l'autorisation de prendre connaissance du contenu de chaque base de données. Tous les systèmes sources ont leurs propres conditions d'autorisation.

LE FACTEUR ORI

Kellie Paquette est la gestionnaire du projet ORI à la GRC. Elle affirme que l'ORI s'est révélé d'emblée un projet stimulant et intéressant. Les équipes d'élaboration et de soutien du projet ont travaillé fort pour régler différents problèmes techniques, allant de l'utilisation d'une plate-forme WebLogic à la coordination avec l'ICP Entrust.

L'un des principaux objectifs de la GRC était d'intégrer les normes de données du RCISP (Réseau canadien d'information pour la sécurité publique) dans l'ORI. Sur le plan de l'interopérabilité, cet objectif représentait tout un défi puisque le SIRP, élaboré à partir d'un logiciel commercial, n'était que partiellement conforme aux normes du RCISP, et que le SRRJ, à titre d'ordinateur central antérieur au RCISP, n'avait absolument aucun rapport avec ces normes.

« L'élaboration de l'élément de transformation des données a débouché sur une série de termes de recherche normalisés dans l'ORI », explique M^me^ Paquette. « Je dirais que 90 % des 125 éléments inclus dans l'ORI sont conformes aux normes. »

Les efforts qu'a faits l'équipe responsable de l'ORI pour se conformer aux normes de données du RCISP ont été soutenus par le Secrétariat de normalisation des données de Sécurité publique et Protection civile Canada.

« L'équipe du Secrétariat de normalisation des données a toujours manifesté beaucoup d'intérêt pour nos travaux », dit M^me^ Paquette, « parce que notre projet est l'un des premiers à se conformer aux normes du RCISP — et aussi l'un des premiers à appliquer ces normes dans un environnement pratique et réel. Grâce à notre expérience, le Secrétariat de normalisation des données a acquis des connaissances qui l'ont aidé à cristalliser le contenu de ses normes, et l'équipe responsable de l'ORI a bénéficié de l'aide active du Secrétariat en matière de normes. »

« C'est une bonne solution », conclut-elle, « car elle n'oblige pas les utilisateurs à changer leurs systèmes sous-jacents. Le SRRJ reste le SRRJ. Le CIPC reste le CIPC. Et maintenant, il y a le SIRP, et vous pouvez interroger ces trois sources d'information en utilisant ce seul outil. Je suis ravie de la réaction des utilisateurs ».

Définir les termes : LES NORMES DE DONNÉES DU RCISP

« Il est important de ne pas oublier que nous sommes en train d'élaborer une norme d'*échange* de données, et non pas une norme de base de données », déclare Alistair Rondeau, gestionnaire au Secrétariat de normalisation des données (SDN). « Autrement dit, nous ne disons pas aux organismes comment ils doivent stocker l'information; nous leur fournissons un cadre et un vocabulaire pour la *mise en commun* de cette information. »

Au cours des 18 derniers mois, le travail sur ce plan s'est déroulé rondement. La version beta finale du dictionnaire des données de base du RCISP a été achevée au début du printemps; la version définitive du document devrait être prête pour l'automne 2004.

« Pour définir les différents éléments de notre dictionnaire de données, nous sommes partis des meilleurs exemples disponibles », explique M. Rondeau. « Par exemple, notre façon de traiter les noms est calquée sur l'approche de Citoyenneté et Immigration Canada, parce que ce ministère est celui qui a le plus d'expérience des noms qui ne suivent pas toujours la formule traditionnelle nord-américaine : prénom, second prénom et nom de famille. »

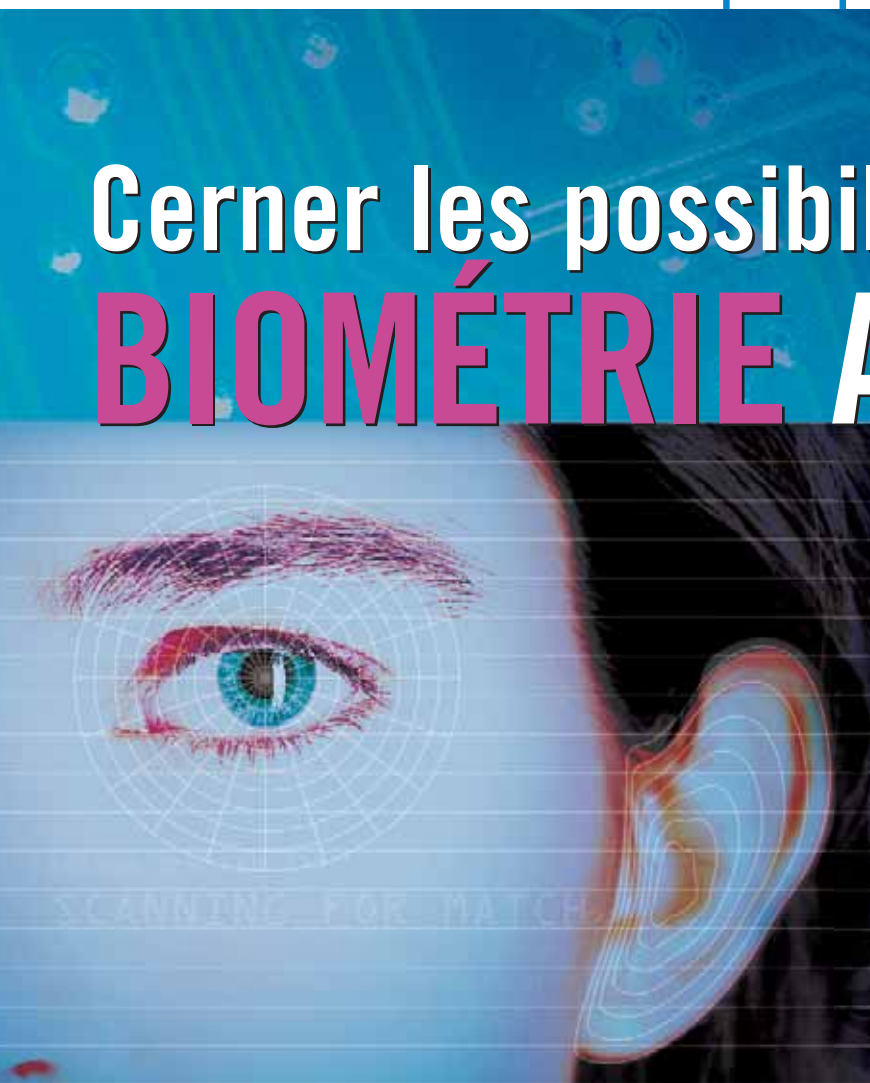
M. Rondeau affirme que de nombreux spécialistes de l'industrie ont félicité le Secrétariat de normalisation des données pour la structure de son dictionnaire des données. Les fournisseurs ont également suivi son élaboration de près, soucieux de s'assurer que leurs solutions répondent aux besoins des ministères qui vont adopter les normes de données du RCISP.

« Nous empruntons une toute nouvelle voie », reconnaît M. Rondeau. « Et le fait que des équipes comme celles d'ORI et de SSDUE (rationalisation de la prestation des services à l'aide de la collaboration électronique) — un autre projet de mise en commun de l'information de la GRC — aient accepté avec enthousiasme de faire route avec nous a été tout simplement formidable. Je suis convaincu que lorsque les gens constateront les avantages de l'échange normalisé de renseignements — et des principes de mise en commun de l'information dont les normes font la promotio nous poserons un jalon important sur le chemin qui conduit à une véritable intégration de l'information de la justice. »

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE :

une importante innovation du secteur des technologies de la sécurité est en train de transformer la sécurité publique et la lutte contre le terrorisme

Cerner les possibilités de la BIOMÉTRIE AU CANADA



CE NE SONT PAS LES *OPINIONS* QUI MANQUENT LORSQU'IL EST QUESTION DE BIOMÉTRIE. TOUT LE MONDE SEMBLE AVOIR UNE IDÉE SUR LE SUJET — ALLANT DE CEUX QUI CROIENT QUE LA BIOMÉTRIE EST LE PLUS GRAND PROGRÈS JAMAIS VU DANS LE SECTEUR DES TECHNOLOGIES DE LA SÉCURITÉ À CEUX QUI CRAIGNENT QUE LA BIOMÉTRIE NE PORTE GRAVEMENT ATTEINTE À LA VIE PRIVÉE.

COMME TOUJOURS, LA VÉRITÉ NE RÉSIDE NI DANS L'UNE NI DANS L'AUTRE DE CES POSITIONS EXTRÊMES. OUI, LA TECHNOLOGIE BIOMÉTRIQUE EST HAUTEMENT PERFECTIONNÉE. OUI, LA PROTECTION DE LA VIE PRIVÉE DOIT ÊTRE PRISE EN CONSIDÉRATION AU MOMENT DE LA CONCEPTION DE SOLUTIONS BIOMÉTRIQUES. MAIS CES SOLUTIONS NE RÉPONDENT PAS COMME PAR ENCHANTEMENT À TOUS LES BESOINS EN MATIÈRE DE SÉCURITÉ ET NE FRANCHISSENT PAS AUTOMATIQUEMENT LES LIMITES CONCERNANT LES RENSEIGNEMENTS PERSONNELS.

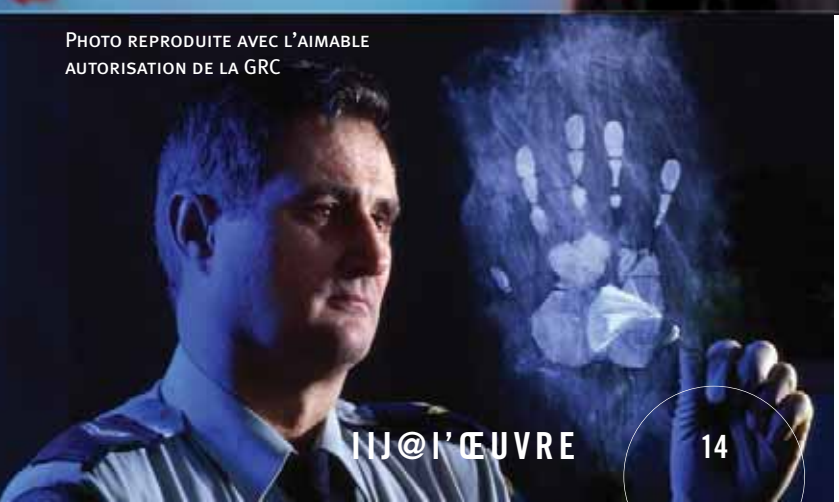


PHOTO REPRODUITE AVEC L'AIMABLE AUTORISATION DE LA GRC

Les différents systèmes biométriques n'ont pas tous le même taux de précision : bien que la question fasse encore l'objet de débats, il est généralement admis que le balayage de l'iris, par exemple, est plus précis que les solutions fondées sur la reconnaissance du visage.

Pour les organismes, les organisations et les gouvernements responsables de la sécurité, la difficulté consiste aujourd'hui à déterminer le véritable potentiel des technologies biométriques et à élaborer des approches pratiques pour les mettre en application.

La tâche n'est pas simple, et il y a de nombreux aspects à prendre en considération. Par exemple, les systèmes biométriques emploient souvent des logiciels privés. Il peut y avoir un manque d'interopérabilité entre les solutions proposées par les fournisseurs. Ainsi, en raison de l'absence de normes d'interopérabilité, une technologie de reconnaissance faciale achetée chez un fournisseur ne permet pas nécessairement de transmettre l'image d'un visage au système venant d'un autre fournisseur. De nombreuses normes potentielles ont été proposées pour les technologies biométriques, mais très peu d'entre elles ont été ratifiées.

La précision est un autre enjeu. Les différents systèmes biométriques n'ont pas tous le même taux de précision : bien que la question fasse encore l'objet de débats, il est généralement admis que le balayage de l'iris, par exemple, est plus précis que les solutions fondées sur la reconnaissance du visage. Et le taux de précision peut varier en fonction de multiples facteurs dont l'un est le degré de contrôle qu'ont les opérateurs de systèmes sur l'environnement dans lequel sont prélevés les échantillons biométriques. La prise des empreintes digitales d'une personne qui se soumet de son plein gré à une vérification de ses antécédents criminels permet de constituer un dossier de meilleure qualité que celui qu'on peut monter en prenant les empreintes digitales d'une personne qui ne veut pas coopérer et qui est accusée d'une infraction. Il est donc impossible d'automatiser entièrement les systèmes biométriques; ils doivent toujours comporter un processus de vérification qui repose sur l'intervention humaine.

En dernier lieu, les systèmes biométriques ne peuvent être utilisés sans qu'on ait au préalable effectué une analyse complète de leurs répercussions sur la protection de la vie privée et sur la législation. C'est un domaine dans lequel il faut procéder lentement et méthodiquement afin de s'assurer de ne pas porter atteinte aux droits à la protection des renseignements personnels dans le simple but d'obtenir un plus haut niveau de sécurité publique.

Le présent article traite de certains des projets de biométrie en cours au Canada, du point de vue des personnes qui en sont responsables. Chaque intervention met en lumière une pièce différente du casse-tête biométrique : depuis les questions stratégiques de haut niveau jusqu'aux difficultés que présente la mise en application d'une solution biométrique particulière.

DÉFINITION DE LA BIOMÉTRIE

Les systèmes biométriques électroniques sont des phénomènes relativement récents, mais la biométrie elle-même a toujours été utilisée par les être humains. Lorsque vous reconnaissez quelqu'un en voyant son visage — en personne ou sur une photo — c'est essentiellement la « biométrie » qui vous permet d'identifier cette personne.

Les technologies biométriques — qui vont des empreintes digitales, du balayage de l'oreille et de l'iris à la reconnaissance faciale et à celle de la géométrie de la main — reproduisent électroniquement ce processus d'identification et d'authentification. (L'authentification consiste à vérifier que la personne reconnue est effectivement celle qu'elle affirme être.)

Pour l'*identification*, les renseignements biométriques individuels obtenus par balayage sont comparés aux renseignements biométriques archivés, dans le cadre d'une recherche injective. Pour l'*authentification*, les données biométriques sont mises en parallèle avec une autre forme d'identification, laquelle sert à confirmer la validité de la première identification. Ce type de recherche comporte une comparaison injective des fichiers.

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE

Entrevue

avec Raj Nanavati concernant l'élaboration des normes de la biométrie

Associé de l'International Biometric Group (IBG), Raj Nanavati est généralement considéré comme une sommité en ce qui concerne l'élaboration des normes de la biométrie. IIJ@l'œuvre a recueilli ses réflexions sur l'état actuel de la situation dans ce domaine — et ce qui pourrait poindre à l'horizon.

Raj Nanavati, partenaire du International Biometric Group

IIJ@l'œuvre : Que pense l'ibg de l'état actuel de l'élaboration des normes de la biométrie?

Raj Nanavati : Il est indéniable que des progrès importants ont été faits. Mais, quant à bon nombre des aspects les plus difficiles à normaliser — tels que le rendement et la précision — il reste encore beaucoup de chemin à parcourir avant de pouvoir considérer la biométrie comme ayant atteint un degré de maturité raisonnable. Le fait que la biométrie soit une discipline aussi jeune, sur la plupart des plans, complique l'élaboration de normes, car celles qui sont adoptées consacrent parfois des technologies et des approches inadéquates.

IIJ@l'œuvre : Qui relève le défi?

RN : En fait, des normes biométriques sont créées par de nombreuses organisations. L'Organisation internationale du travail (OIT). L'Organisation de l'aviation civile internationale (OACI). Le National Institute of Standards in Technology (NIST). L'ISO et la CEI (l'Organisation internationale de normalisation et la Commission électrotechnique internationale). Ces organisations s'intéressent à différents éléments biométriques : les empreintes digitales, le visage, l'iris.

IIJ@l'œuvre : Alors, cela soulève une autre question : comment rationaliser ces normes?

RN : En maintenant des relations de liaison par l'entremise des comités JTC1 de l'ISO et de la CEI. En particulier, le travail technique effectué par l'OIT et l'OACI est aligné avec celui des comités concernés, dont les suivants : SC 37 (biométrie), SC 17 (cartes et documents d'identification personnelle) et SC 27 (techniques de sécurité des technologies de l'information). Il s'agit d'un processus qui exige beaucoup de temps, mais ces groupes estiment que l'alignement de leurs formats et de leurs interfaces sera profitable à long terme.

IIJ@l'œuvre : Que pensez-vous des taux de précision de la biométrie et de l'impact que peuvent avoir les installations à grand volume dans les aéroports et dans les postes frontaliers?

RN : À vrai dire, cette question nécessite une longue analyse. Pour vous donner une réponse très générale, on pourrait dire que la précision sera beaucoup moins touchée par les détails pratiques des algorithmes et les devis descriptifs des capteurs que par des choses comme l'intégration dans le flux des travaux, la formation et la motivation de l'utilisateur final. Le volume d'une installation n'a rien à voir avec les taux de précision — à moins qu'il ne s'agisse d'une application d'*identification*.

D'après les résultats obtenus à ce jour avec US VISIT (l'indicateur américain du statut de visiteur et d'immigrant), la précision des empreintes digitales a été « suffisamment bonne » pour répondre aux besoins des inspecteurs. Surtout parce qu'en plus des données biométriques, les inspecteurs ont maintenant accès à d'autres sources de renseignements sur les visiteurs, en particulier à la Consular Consolidated Database. Si la CBP (la patrouille douanière et frontalière américaine) réussit à maintenir le temps moyen nécessaire pour éliminer les fausses concordances autour d'une minute et sept secondes, comme il a été mentionné à l'audience de la Chambre en janvier, le rendement de la biométrie en soi risque beaucoup moins de devenir un enjeu. Cependant, on ne sait pas encore si les débits de traitement actuels pourront être maintenus au fur et à mesure qu'augmentera la taille de la base de données de US VISIT, car la saison estivale des voyages approche, et l'on est en train d'installer le système US VISIT aux points d'entrée terrestres.

IIJ@l'œuvre : Que pensez-vous des efforts déployés pour créer des modèles normalisés pour les échanges de renseignements biométriques et l'interopérabilité? Un modèle normalisé ne supprime-t-il pas la capacité concurrentielle des fournisseurs de logiciels privés?

RN : En réalité, la question peut être en partie formulée ainsi : les modèles ou les images normalisés nuisent-ils à la capacité des fournisseurs d'apparier une lecture biométrique directe avec des données biométriques archivées? D'une façon ou d'une autre, les données disponibles ne sont pas suffisantes pour que nous le sachions. À vrai dire, non seulement aucun essai n'a été effectué à cet égard, mais les experts ne s'entendent pas vraiment sur la manière de s'y prendre pour mesurer les facteurs concernés. Dans le domaine des systèmes informatisés de dactyloscopie, où des normes d'image de l'interopérabilité ont été élaborées, le recours à la technologie a donné de bons résultats. Il peut en être tout autrement des modèles normalisés. Dans bien des cas, ils favorisent fortement un fournisseur ou une approche.

IIJ@l'œuvre : Vous avez mentionné les systèmes informatisés de dactyloscopie. À l'heure actuelle, qu'en est-il exactement des normes dactyloscopiques?

RN : Il existe au moins deux méthodes pour comparer les empreintes digitales : la concordance basée sur les particularités et celle basée sur les formes. La première est souvent perçue comme mieux adaptée aux applications traditionnelles, là où le volume des empreintes digitales est important. Il en est ainsi par exemple dans le marché judiciaire des systèmes informatisés de dactyloscopie. Les systèmes basés sur les particularités y sont prédominants. Les algorithmes basés sur les formes semblent convenir davantage aux applications comportant un volume moins considérable d'empreintes digitales. Mais il n'y a pas d'interopérabilité entre les deux formes de concordance. Et les fournisseurs de chaque catégorie de solutions affirment généralement que leur approche est plus précise.

Dans l'industrie, certains se demandent si les solutions de concordance basée sur les formes seront un jour soumises à des essais suffisamment poussés pour qu'on puisse les comparer aux solutions basées sur les particularités. En fin de compte, le choix sera fonction des besoins opérationnels. La concordance basée sur les formes est probablement « suffisamment bonne » lorsqu'une solution est axée principalement sur la vitesse de traitement et une précision de « un pour un », plutôt que sur la chaîne de production visant à trouver « une aiguille dans une botte de foin », comme celle que permettent les systèmes informatisés de dactyloscopie.

Alors, pour revenir à la question : dans la conception d'images et de modèles normalisés on cherche à rendre possible l'interopérabilité des systèmes et des sphères de compétence. Les normes de concordance basée sur les formes suscitent beaucoup de controverse, car il est impossible de concilier un si grand nombre d'approches différentes à l'aide d'une seule norme.

IIJ@l'œuvre : Cette réflexion touche à une question plus générale et plus pressante, à savoir ce qu'il faut faire pour recueillir des renseignements biométriques qui seront acceptables sur le plan international.

RN : Il est peu probable, et pas nécessaire non plus, qu'il faille recueillir une seule donnée biométrique pour assurer l'intégrité des frontières internationales. Dans les cas où un voyageur doit se procurer un visa avant de se présenter à une frontière pour inspection, le pays qui délivre ce visa peut exiger une donnée biométrique de son choix pour protéger le document. Pour les voyages sans visa — comme ceux rendus possibles par le Programme de dispense de visa — les pays participants n'ont qu'à convenir de s'échanger *les outils nécessaires pour décoder et vérifier la concordance* de renseignements biométriques sur un voyageur, dans le même format que celui utilisé par le pays de délivrance.

Les gens se demandent si l'utilisation de renseignements biométriques se butte à des barrières culturelles : par exemple, certains groupes ont-ils une aversion pour la prise d'empreintes digitales ou le balayage de l'iris? Les résultats obtenus à ce jour dans le cadre du programme US VISIT donnent à penser que ces objections sont beaucoup moins problématiques que prévu. Se rendre dans un autre pays demeure un privilège, pas un droit, et les visiteurs font preuve de beaucoup de patience et de retenue, tant et aussi longtemps que les mesures sont jugées raisonnables. Le programme US VISIT s'est révélé relativement efficace. Il s'applique à tous les détenteurs de visa et semble considéré comme une mesure de sécurité raisonnable. Je crois que la « barrière culturelle » deviendra vite un faux problème si les gens estiment que les postes frontaliers sont efficaces et bien administrés.

VUE D'ENSEMBLE

La nouvelle politique canadienne de sécurité nationale met en lumière les technologies biométriques

L'IDÉE D'UTILISER LE BALAYAGE DU VISAGE, DE L'IRIS OU DES EMPREINTES DIGITALES DANS LES DOCUMENTS DE VOYAGE OU AUX POSTES FRONTALIERS SEMBLAIT AUPARAVANT SORTIE TOUT DROIT DES FILMS, MAIS, EN UN PEU PLUS DE DEUX ANS, LES TECHNOLOGIES BIOMÉTRIQUES SONT PRATIQUEMENT DEVENUES LE MOYEN IDÉAL DE CONFIRMER L'IDENTITÉ DES VOYAGEURS ET DES AUTRES PERSONNES EN DÉPLACEMENT[1].

À la fin d'avril 2004, dans le cadre de sa nouvelle politique de sécurité nationale, le gouvernement du Canada a annoncé qu'il commencera à délivrer, dès le début de 2005, des passeports dans lesquels auront été intégrées des puces contenant des renseignements biométriques. Il a également annoncé qu'il dépenserait près de 100 millions de dollars pour améliorer sa capacité de filtrage de données électroniques sur les empreintes digitales. En fait, dans la nouvelle politique de sécurité nationale, le gouvernement s'engage à utiliser plus largement la biométrie, car il s'est aperçu que « la communauté internationale recourt de plus en plus aux nouvelles technologies, dont la biométrie[2] », pour améliorer la sécurité.

Après les événements du 11 septembre 2001, le gouvernement fédéral a offert aux voyageurs de leur procurer volontairement des cartes d'identité biométriques et a installé des kiosques de balayage de l'iris dans les principaux aéroports[3]. Parallèlement, le gouvernement lançait d'autres initiatives biométriques, dont celle de la carte de résident permanent, et collaborait activement avec l'Organisation de l'aviation civile internationale (OACI) à l'élaboration de normes de sécurité mondiales interopérables fondées sur la reconnaissance faciale pour l'établissement des documents de voyage.

Mais les ministères et organismes fédéraux qui envisagent d'utiliser la biométrie pour améliorer la sécurité doivent commencer par répondre à un certain nombre de questions très importantes. Par exemple, dans quel cadre de travail les solutions biométriques

[1] Staples, Sarah. « Red-Hot Cybersecurity: Biometrics, shared databases create virtual borders », *Ottawa Citizen*, le 6 mai 2004, p. G1 et G3.

[2] *Protéger une société ouverte : la politique canadienne de sécurité nationale*, avril 2004, p. 45, www.pco-bcp.gc.ca.

[3] Staples, Sarah. « Red-Hot Cybersecurity: Biometrics, shared databases create virtual borders », *Ottawa Citizen*, le 6 mai 2004, p. G3.

peuvent-elles être appliquées au Canada? À quel moment une technologie biométrique est-elle la plus appropriée pour améliorer la sécurité? Quelles sont les prochaines étapes?

Dernièrement, une équipe d'ingénieurs du gouvernement du Canada, au Centre de la sécurité des télécommunications (CST), a pris des mesures pour tenter de répondre à ces différentes questions. Entre septembre 2003 et mars 2004, le gouvernement du Canada a produit deux documents s'appuyant sur les résultats d'enquêtes effectuées auprès de neuf ministères et organismes fédéraux[4]. Le premier document s'intitule *Biometrics Business Requirements Report* et le second *Government of Canada Identification and Authentication Framework for Biometric Enabled Applications*. Les exigences opérationnelles et le cadre de travail visent à aider les organismes à évaluer la viabilité des options biométriques en fonction de leurs besoins.

UNE PERSPECTIVE RÉALISTE

Les rapports ne contiennent pas beaucoup de renseignements sur les exigences opérationnelles des différentes technologies biométriques; ils portent principalement sur les technologies qui pourraient être utilisées dans un système réel, déployable. Le mandat du Centre de la sécurité des télécommunications est de fournir des avis et conseils techniques au gouvernement fédéral sur des questions concernant les technologies de la sécurité ainsi que sur des solutions techniques qui pourraient être adaptées aux besoins de chacun des ministères.

Les exigences opérationnelles sont définies en fonction des objectifs, de l'environnement et des questions relatives à l'intégration : *Qu'est-ce que la* biométrie est censée permettre de réaliser? *Où* les technologies biométriques seront-elles déployées? *Comment* les technologies biométriques seront-elles incorporées dans les systèmes existants?

« Dans un système sécurisé, la biométrie n'est qu'un mécanisme possible d'authentification parmi d'autres », explique Drew Smeaton, directeur technique de la biométrie au CST. « La méthode choisie doit correspondre aux normes de sécurité des applications utilisées par un organisme ou un ministère, et favoriser une approche globale de la sécurité. »

L'équipe du CST reconnaît qu'il n'existe pas d'approche uniformisée, et que les particularités de toute solution biométrique découlent des besoins fonctionnels de l'organisation concernée. « La biométrie n'existe pas en situation isolée et ne peut être abordée de cette manière », dit M. Smeaton. C'est ici que le document *Government of Canada Identification and Authentication Framework* prend tout son sens en établissant, au moment d'élaborer des solutions, des paramètres qui s'articulent autour des exigences opérationnelles.

UNE PREMIÈRE ÉTAPE

Les documents publiés récemment par le gouvernement du Canada sont censés être les premiers d'une série de publications sur le sujet. Ils décrivent la nécessité d'étudier les technologies disponibles, de définir les besoins fonctionnels particuliers et d'analyser les aspects stratégiques des étapes suivantes. « Il y a encore beaucoup de questions stratégiques à examiner en ce qui concerne les interfaces, la communication de renseignements biométriques et la protection de la vie privée », rappelle M. Smeaton.

Au cours des prochains mois, le gouvernement lancera des initiatives dans le secteur de la biométrie, conformément aux normes internationalement acceptées; il y aura sûrement des questions stratégiques à résoudre. Durant ce temps, l'équipe d'ingénieurs du CST a l'intention de continuer d'explorer les exigences techniques de la mise en application de technologies biométriques à l'intérieur du gouvernement du Canada. « Nous voulons être en mesure d'exposer clairement le point de vue technique afin de faciliter la prise de décisions lorsque des questions stratégiques seront soulevées. »

DIX EXIGENCES FONCTIONNELLES LIÉES À L'ACTIVITÉ BIOMÉTRIQUE

Dans le domaine de l'activité biométrique, les exigences fonctionnelles du gouvernement du Canada seraient les suivantes :

1. Besoin commun d'identification des personnes à l'aide de papiers d'identité non partageables
2. Besoin commun de confirmer, avec un haut degré de certitude, cette identification
3. Approche prudente de la mise en application de la biométrie (technologie, protection de la vie privée, acceptation par les utilisateurs, etc.)
4. Détermination des taux d'erreur et de traitement acceptables, selon les environnements d'application
5. Prise en considération des besoins particuliers de l'industrie en ce qui concerne la rétrocompatibilité avec les systèmes existants d'analyse des caractéristiques humaines
6. Prise en considération de la portée et de l'envergure des projets (l'envergure des projets varie d'un palier de gouvernement à l'autre, et les utilisateurs peuvent être des centaines, des milliers, voire des millions)
7. Intégration de services d'identification et d'authentification biométriques dans différents scénarios de déploiement d'applications et de contrôles d'accès physique
8. Intégration de services d'identification et d'authentification dans différents scénarios de déploiement de modèles de sécurité en prêtant une attention particulière à l'interopérabilité des infrastructures à clé publique
9. Processus de vérification et d'attestation visant à confirmer que les produits reposant sur la biométrie sont efficaces et respectent les normes acceptées
10. Prise en considération des politiques et normes dans toute l'administration fédérale

— *Texte adapté du* Biometrics Business Requirements Report, *paru le 9 mars 2004, CST*

[4] Transports Canada, l'Agence des services frontaliers du Canada, le Conseil privé, le Service correctionnel du Canada, le Secrétariat de l'IIJ, la GRC, l'Administration canadienne de la sûreté du transport aérien, le ministère des Affaires étrangères et du Commerce international, et Citoyenneté et Immigration Canada.

MISE À L'ESSAI –

La biométrie faciale est-elle à la hauteur?

Le Bureau des passeports du Canada répond à la question

Jocelyn Francœur, arbitre et ombudsman au Bureau des passeports du Canada

En mai 2003, l'Organisation de l'aviation civile internationale (OACI) a demandé que des renseignements biométriques soient intégrés dans les passeports et recommandé que la norme soit la reconnaissance faciale.

« C'est logique », dit Jocelyn Francœur, arbitre et ombudsman au Bureau des passeports du Canada. « Après tout, le passeport contient déjà une image du visage de la personne. Il n'est pas très difficile de songer à utiliser la technologie de la reconnaissance faciale pour vérifier l'identité du détenteur du passeport et établir un lien avec la photo intégrée dans le document. »

Dans le contexte de vérifications injectives, la précision et l'efficacité de la technologie de la reconnaissance faciale ont cependant été remises en question. Aux États-Unis, des tests effectués par le National Institute for Standards in Technology (NIST) ont donné des résultats mitigés.

Les organismes centraux du Canada voulaient vérifier eux-mêmes l'efficacité de cette technologie. Étant donné que le Bureau des passeports possède déjà une base de données de centaines de milliers d'images faciales, il s'est porté volontaire pour diriger l'étude.

ABSENCE DE PRÉSOMPTION

« Nous n'avions pas décidé d'utiliser la technologie de la reconnaissance faciale », dit M. Francœur, qui a dirigé le projet de recherche dans une perspective indépendante. « Et aucun autre organisme n'avait pris de décision à cet égard. Nous n'avions pas de parti pris concernant les essais; si la technologie de la reconnaissance faciale échouait, tant pis. Il n'y avait pas d'enjeu pour nous. »

Après avoir obtenu le financement nécessaire pour effectuer l'essai pilote et préparer le dossier de l'analyse de rentabilisation de la technologie de la reconnaissance faciale, le Bureau des passeports a entrepris d'élaborer une méthodologie susceptible de donner des résultats pratiques et pertinents. Cette méthodologie (inspirée des modèles existants) consistait à comparer des paires d'images : à prendre deux photos différentes de la même personne et à déterminer si les technologies disponibles actuellement permettaient d'établir une concordance entre les deux avec un degré élevé de certitude.

« Des essais antérieurs avaient permis d'examiner entre 500 et 1 000 paires d'images », explique M. Francœur. « Nous avons utilisé plus de 6 000 paires d'images. C'est le plus grand nombre d'images jamais employé pour ce genre d'essai. Et nous avons ajouté du « bruit » pour que notre essai ressemble davantage au monde réel. Il n'y avait pas seulement 6 000 paires d'images; 143 000 autres images individuelles faisaient partie de la base de données de l'essai. »

C'est pour une raison pratique que l'essai a été effectué à une si grande échelle. Le Bureau des passeports traite plus de 2 000 000 de demandes par année. Dans un environnement de reconnaissance faciale, chacune des photos mises en correspondance doit être comparée à des photos de personnes dont les noms figurent sur les listes de surveillance des services de sécurité.

« Le système biométrique dont nous faisions l'étude pouvait être utilisé dans un mode de comparaison injectif, ce qui n'est pas le cas lorsque la photo est enregistrée sur une puce — laquelle est ensuite insérée dans un passeport et rend possible une comparaison d'un pour un », fait observer M. Francœur.

COEFFICIENT ÉLEVÉ DE CONFIANCE

Le Bureau des passeports a fait examiner et valider sa méthodologie par le Département de mathématiques et de statistiques de l'Université d'Ottawa. La taille de l'échantillon d'images utilisé a permis d'obtenir des résultats dont le coefficient de confiance s'élevait à 99,7 %.

« Les résultats de l'essai eux-mêmes étaient assez positifs, s'échelonnant de 75 % à plus de 90 % selon la qualité des images et la taille des archives auxquelles elles étaient comparées », dit M. Francœur. « Encore une fois, cela est révélateur de notre approche. Chacun des fournisseurs d'une technologie de reconnaissance faciale qui participaient à notre projet disposait de dix jours pour améliorer ses processus, ses algorithmes et autres mécanismes semblables. Ce délai est tout à fait réaliste. Lors d'une mise en application dans le monde réel, aucun fournisseur ne disposerait de quelques heures seulement pour trouver une solution à un problème. Il faut prévoir une phase d'ajustement à la difficulté particulière. En fait, nous avons mesuré la meilleure application de la technologie dans les circonstances les plus exigeantes qu'il nous était possible de simuler. »

Selon M. Francœur, le taux élevé de concordance peut s'expliquer aussi par le fait que les photos de passeport se prêtent particulièrement bien à l'utilisation de la technologie de la reconnaissance faciale, car elles sont prises dans des conditions contrôlées et doivent satisfaire à une norme définie de qualité.

« Il vous faut de bonnes photos », dit-il. « Plus les photos sont de bonne qualité, plus la solution proposée va donner de bons résultats. »

PROTECTION DE LA VIE PRIVÉE

Comme les autres technologies biométriques, la reconnaissance faciale consiste à transformer une photo — dans le cas présent, celle d'un visage humain — en un identificateur alphanumérique appelé modèle. (Lorsque les gens font mention de l'inclusion d'un renseignement biométrique dans leur passeport, ils parlent de l'enregistrement de la photo sur une puce.) Le modèle lui-même n'est pas enregistré sur le passeport et ne contient pas non plus de renseignements personnels.

« Il y a davantage de renseignements personnels sur votre permis de conduire que dans un modèle biométrique », dit M. Francœur. « En fait, le modèle est tout à fait anonyme ». Dans son essai, le Bureau des passeports a appliqué les quatre critères du Commissaire à la protection de la vie privée pour déterminer les répercussions des technologies biométriques et d'autres mesures de sécurité sur le plan de la vie privée. Ces critères sont les suivants :

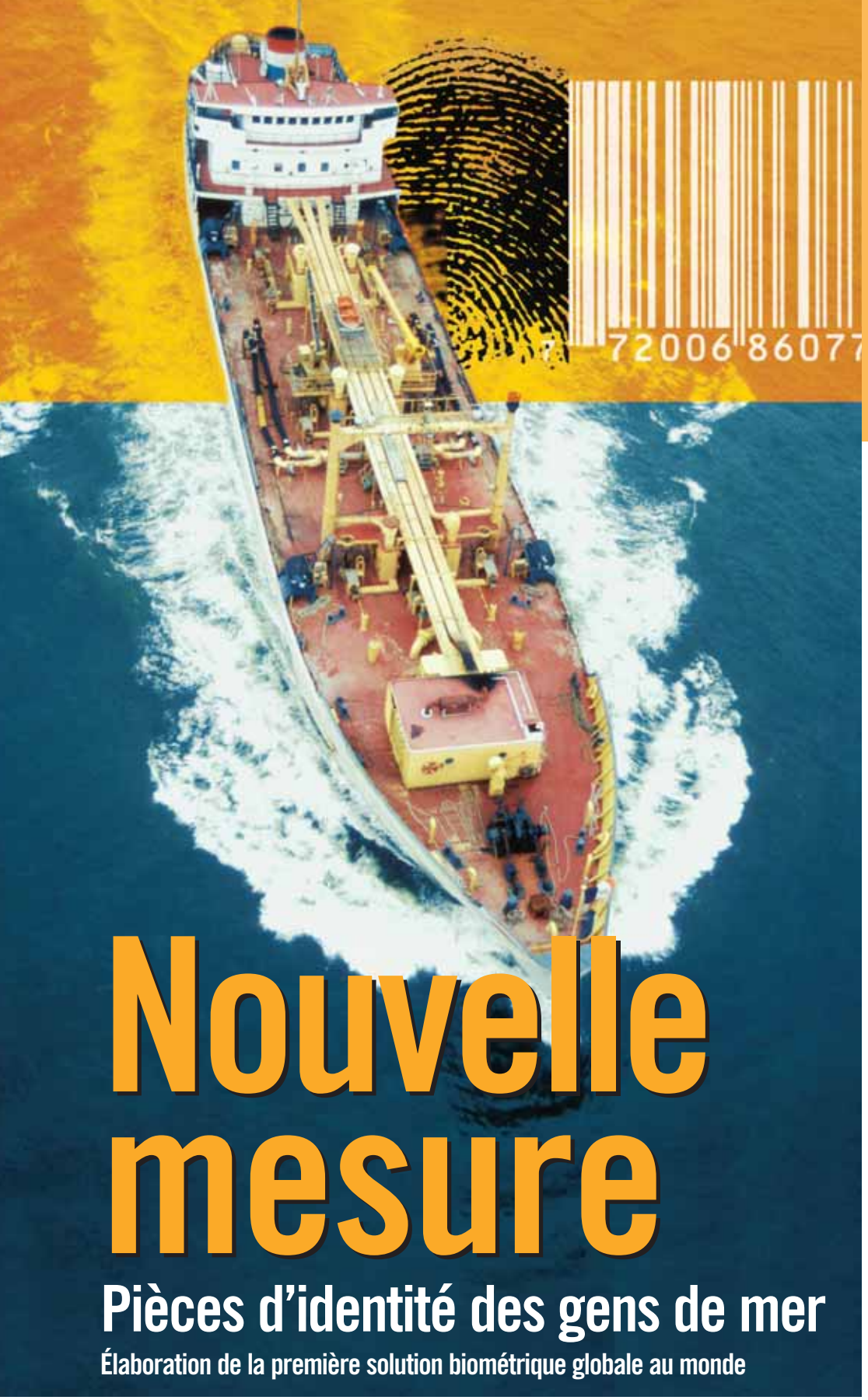
1. la mesure est manifestement nécessaire pour répondre à certains besoins;
2. tout indique que la mesure sera probablement efficace pour satisfaire les besoins à l'origine du déploiement proposé;
3. l'ingérence dans la vie privée est proportionnelle à l'avantage en matière de sécurité;
4. il peut être montré qu'aucune autre mesure comportant une ingérence moindre dans la vie privée ne permettrait d'atteindre les mêmes résultats.

Encore une fois, M. Francœur et son équipe sont d'avis que la technologie respecte ces quatre principes puisque les photos sont déjà exigées pour les passeports et que le modèle biométrique en soi est anonyme.

LE FACTEUR HUMAIN

Bien entendu, l'apparence d'une personne se transforme légèrement entre le moment où une photo est prise et celui où elle se fait de nouveau photographier. Et cela signifie que la séquence alphanumérique générée pour la même personne sera différente à chaque occasion.

SUITE À LA PAGE 44



Nouvelle mesure

Pièces d'identité des gens de mer

Élaboration de la première solution biométrique globale au monde

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE

PLUS D'UN MILLION DE GENS DE MER SILLONNENT LES MERS AUJOURD'HUI — DES HOMMES ET DES FEMMES AU SERVICE DE L'INDUSTRIE DES TRANSPORTS MARITIMES. CETTE INDUSTRIE EST RESPONSABLE DE LA CIRCULATION DE PLUS DE 70 % DES BIENS COMMERCIAUX DANS LE MONDE; AUTREMENT DIT, IL S'AGIT D'UNE INDUSTRIE ÉCONOMIQUEMENT ESSENTIELLE.

Depuis 1958, les gens de mer peuvent se procurer une pièce d'identité des gens de mer. Délivré par les États membres de l'Organisation internationale du travail (OIT), ce document vise à faciliter aux gens de mer l'entrée dans les pays membres de l'OIT lors d'une permission à terre, d'un transit, d'un transfert ou d'un rapatriement.

En juin 2003, réagissant aux préoccupations en matière de sécurité à la suite des attaques terroristes du 11 septembre 2001, l'OIT a adopté une convention qui apportait une modification à la pièce d'identité des gens de mer. L'objectif : renforcer les aspects relatifs à la sécurité de la pièce d'identité des gens de mer et veiller à ce qu'elle demeure un document professionnel tout en devenant un document contenant des renseignements attestés. Cette modification fera de la pièce d'identité des gens de mer la première solution biométrique globale au monde.

Donald Roussel, directeur de Normes du personnel maritime et pilotage à Transports Canada, est chargé du dossier des pièces d'identité des gens de mer dans ce pays. Il a donc une vision très personnelle du processus mis en branle pour trouver une solution à une si grande échelle.Donald Roussel, directeur de Normes du personnel maritime et pilotage à Transports Canada, est chargé du dossier des pièces d'identité des gens de mer dans ce pays. Il a donc une vision très personnelle du processus mis en branle pour trouver une solution à une si grande échelle.

CRÉATION D'UN CONSENSUS

« Le premier défi que devait relever l'OIT », rappelle M. Roussel, « était de trouver un

renseignement biométrique qu'on pouvait utiliser dans tous les pays membres du monde, en tenant compte des facteurs technologiques, des disparités économiques et des questions ayant trait à l'interopérabilité. Ce seul objectif constituait en soi une tâche colossale. »

Après l'examen de ces différents aspects, ce sont les empreintes digitales qui ont été retenues pour la pièce d'identité des gens de mer, car la dactyloscopie est déjà utilisée de façon assez courante, est assez simple et coûte relativement peu cher.

Il fallait ensuite tenir compte des préoccupations et des attentes d'un groupe d'étude tripartite.

« Étant donné que la pièce d'identité des gens de mer est le produit d'une convention internationale du travail, les travailleurs, les employeurs et les gouvernements ont travaillé ensemble à déterminer le mode d'utilisation du nouveau document comportant des caractéristiques biométriques. »

Voici comment est utilisée la nouvelle pièce d'identité des gens de mer : les empreintes digitales du marin sont balayées et transformées en une séquence numérique, laquelle est ensuite imprimée, sous forme de code à barres, dans la pièce d'identité elle-même. En soi, cette séquence numérique est totalement anonyme, et aucun renseignement ne peut y être ajouté une fois qu'elle est imprimée.

« Encore aujourd'hui, beaucoup de mystère entoure les renseignements biométriques », dit M. Roussel. « Certains craignent que l'information figurant sur la pièce d'identité des gens de mer ne soit utilisée pour reproduire les empreintes digitales d'une personne, mais ce n'est tout simplement pas le cas. L'identificateur biométrique que contient le code à barres n'est pas une *représentation* des empreintes digitales; ce n'est qu'un modèle ou une série de chiffres. D'autres redoutent une intrusion dans la vie privée d'une personne. Mais la méthode de stockage des renseignements biométriques dans la pièce d'identité des gens de mer fait en sorte que cette information ne puisse être modifiée ou utilisée sans le consentement du titulaire de la carte.

FORMAT NORMALISÉ

Le modèle de sécurité de la pièce d'identité des gens de mer est sensiblement de même taille et de même forme que celui d'un passeport, et il est conforme aux normes de l'OACI pour un document de ce genre. Chaque pièce d'identité porte un numéro unique attribué par le pays qui l'a délivrée. En plus de données biométriques en code à barres, cette pièce d'identité contient une photo numérique ainsi que des renseignements de base tels que le nom de l'autorité compétente, le nom au complet du titulaire de la carte ainsi qu'une date d'expiration.

En pratique, la pièce d'identité des gens de mer doit être présentée aux autorités portuaires ou aux fonctionnaires des douanes dans les pays membres de l'OIT. Ceux-ci utiliseront un appareil spécial qui lit l'information biométrique (les chiffres du code à barres) et établiront une concordance avec les empreintes digitales du marin prélevées en direct. Ils seront ensuite en mesure de vérifier l'authenticité et la validité de la pièce d'identité, soit électroniquement ou en communiquant avec un « centre de liaison » dans le pays émetteur. L'autorité compétente de chacun des pays doit offrir des services de vérification 24 heures sur 24 et sept jours sur sept. Au Canada, Transports Canada sera l'autorité chargée de délivrer les nouvelles pièces d'identité des gens de mer, comme il le fait déjà pour la version antérieure de ces documents. Ce ministère a l'intention de gérer l'ensemble du processus à l'interne.

« Nous possédons les installations nécessaires pour produire les pièces d'identité des gens de mer », affirme M. Roussel. « Si nous devions délivrer de telles pièces d'identité à tous les gens de mer au Canada, leur nombre s'élèverait à quelques 30 000 cartes au total. C'est un volume de documents que Transports Canada peut gérer de manière sûre et efficace. » M. Roussel ajoute qu'il a pour ambition de délivrer de nouvelles pièces d'identité à tous les gens de mer canadiens — et souhaite, qu'en fin de compte, ce document devienne une carte d'identité obligatoire pour tous les gens de mer du monde.

« La convention est volontaire », fait-il observer, « et l'a toujours été. Les gens de mer doivent avoir un passeport sur eux lors d'un transit, mais ils ne sont tenus pour l'instant d'être également titulaires de la pièce d'identité des gens de mer. Mais il y a des avantages à posséder les deux documents — tant pour les gens de mer que pour les autorités frontalières. Pour les gens de mer, cette pièce d'identité professionnelle accélère le processus d'entrée dans les pays membres de l'OIT lorsqu'ils sont en permission à terre ou en transit. Pour les autorités frontalières, elle constitue une mesure de sécurité supplémentaire et rassurante. »

CE QUI SE PROFILE À L'HORIZON

La nouvelle convention sur l'identification des gens de mer (C-185) entrera en vigueur six mois après la date à laquelle sa ratification par deux membres aura été signifiée au directeur général de l'OIT. Autrement dit, il n'y a pas de date fixe. Mais M. Roussel s'attend à ce que cela se fasse au cours des 12 prochains mois.

Entre-temps, le Canada a encore des préparatifs à faire. Transports Canada doit autoriser officiellement la délivrance des pièces d'identité des gens de mer, et il faut constituer une base de données nationale des gens de mer inscrits. En outre, l'Agence des services frontaliers du Canada et Citoyenneté et Immigration Canada doivent se préparer à traiter les pièces d'identité portant des renseignements biométriques que présenteront les gens de mer internationaux qui veulent entrer au Canada.

M. Roussel est fier du travail accompli à ce jour concernant les pièces d'identité des gens de mer et il est également confiant que cette première solution globale biométrique atteindra ses objectifs.

« Dans le secteur de la biométrie, la technologie est imposante et il y a beaucoup de normes à respecter. Mais pour l'instant, la convention sur l'identification des gens de mer est le seul programme à avoir été accepté par un grand nombre de pays par l'entremise d'une organisation internationale. Il s'agit de la première solution biométrique réellement globale au monde; elle permet d'améliorer la sûreté maritime tout en répondant aux besoins de l'industrie contemporaine des transports maritimes dans une économie mondiale.

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE

IDENTIFICATION PAR L'IRIS

CANPASS-Air simplifie les formalités douanières pour les grands voyageurs

La plupart des voyageurs comprennent la nécessité d'appliquer des mesures de sécurité rigoureuses dans les aéroports, mais, à vrai dire, ceux qui prennent souvent l'avion n'apprécient pas toujours le fait de devoir à chaque fois se soumettre au processus d'inspection. Et derrière le comptoir, la majorité des agents de douane et d'immigration conviennent que leur temps est mieux utilisé lorsqu'ils s'occupent des voyageurs inconnus qui peuvent présenter un risque plus élevé que des voyageurs bien connus, à faible risque.

Ces deux facteurs sont au cœur même du programme CANPASS-Air. CANPASS-Air est une initiative conjointe de l'Agence des services frontaliers du Canada (ASFC) et de Citoyenneté et Immigration Canada (CIC); elle facilite l'entrée rapide et en toute sécurité au Canada des voyageurs préautorisés qui utilisent les transports aériens et qui présentent un risque peu élevé. La clé? Un système biométrique de balayage de l'iris qui confirme avec précision et instantanément l'identité des participants au programme.

CONSTATATION DU BESOIN

Aileen Dimasuay est agente principale du projet CANPASS-Air à l'ASFC. Elle explique que le choix de la technologie de la reconnaissance de l'iris s'est appuyé sur quatre critères. En particulier, la solution biométrique retenue devait :

1. Être **sûre** — quelque chose qui ne peut être perdu ou volé.
2. Être utilisable avec la **technologie disponible à l'heure actuelle**.
3. Être **précise**.
4. Permettre des **identifications rapides** de manière **discrète**.

Après avoir établi que la technologie de la reconnaissance de l'iris répondait à ces quatre critères, les responsables du programme CANPASS-Air ont ouvert un premier centre d'inscription à l'aéroport de Vancouver en mars 2003. Huit mois plus tard, un deuxième centre d'inscription était établi à l'aéroport international d'Halifax.

LE MODE DE FONCTIONNEMENT DE CANPASS-AIR

Le système CANPASS-Air enregistre une image photographique des iris d'un voyageur. (Les deux yeux sont utilisés parce que chaque œil est unique — ce qui rend ce renseignement biométrique encore plus sûr.) Cette image est encodée et stockée dans une base de données sécurisée, gérée par l'ASFC. Lorsqu'une personne inscrite au programme arrive au Canada après un vol international, elle se rend à un kiosque libre-service, équipé d'un appareil photo numérique : l'appareil prend une photo des iris du participant au programme et la compare à celle conservée au dossier.

Le voyageur doit répondre à certaines questions — devant l'écran du kiosque. Le système vérifie l'identité du participant, puis imprime un reçu que ce dernier présente à l'agent à la sortie de la salle des douanes. Pour les besoins de la vérification de

l'observation, les voyageurs peuvent aussi être invités à sortir des rangs pour se soumettre à une inspection au hasard.

« Si CANPASS-Air est aussi précis et aussi fiable, c'est parce que le système n'accepte que l'image d'un iris captée en direct », explique M^me^ Dimasuay. « Par exemple, vous ne pouvez pas jouer d'astuce en présentant une photo à la caméra. Le système relève la profondeur et certaines dimensions importantes, puis établit une comparaison avec le modèle d'iris déjà stocké dans une banque de données. »

M^me^ Dimasuay estime que ce qui rend CANPASS intéressant, c'est en partie le fait qu'il soit, à bien des égards, axé sur les besoins des consommateurs.

« CANPASS-Air est un programme facultatif pour les grands voyageurs », dit-elle. « Ce programme accélère les formalités douanières pour ces personnes. Par ailleurs, en sortant les voyageurs « préautorisés » de la file d'attente, CANPASS-Air permet aux agents de porter leur attention sur les voyageurs inconnus. »

Actuellement accessible aux citoyens et résidents permanents du Canada et des États-Unis, le programme CANPASS-Air pourrait être étendu prochainement à d'autres pays n'exigeant pas de visa ainsi qu'aux voyageurs d'affaires visés par l'Accord de libre-échange nord-américain. À ce jour, environ 3 000 personnes se sont inscrites à ce programme.

En conformité avec l'objectif principal de répondre aux besoins des consommateurs, la promotion de CANPASS-Air a été faite dans les aéroports et sur les sites Web des aéroports, dans les publications sur les voyages telles les revues *En Route* et *Bon Voyage*, et dans des annonces publiques.

UNE VÉRIFICATION RIGOUREUSE

Sur le plan de la sécurité, l'efficacité de CANPASS-Air découle en partie de l'utilisation d'un système biométrique de balayage de l'iris et en partie de la rigueur de son processus de vérification des participants. Ces personnes doivent remplir un formulaire de demande, font l'objet d'une évaluation du risque comportant une recherche dans cinq bases de données constituées par des organismes d'application de la loi et doivent se soumettre à une entrevue personnelle approfondie au centre d'inscription — tout cela avant l'enregistrement des renseignements biométriques et l'obtention d'une carte CANPASS-Air. (Cette carte contient des renseignements d'identification personnelle et une photo numérique.) Les droits d'adhésion au programme sont fixés à 50 $ par année.

ALLER DE L'AVANT

Plus tard en 2004, le programme sera étendu à toutes les régions du pays, et des centres d'inscription seront ouverts dans les aéroports suivants :

- Aéroport international Lester B. Pearson, à Toronto – juin 2004
- Aéroport international de Calgary – automne 2004
- Aéroport international d'Edmonton – automne 2004
- Aéroport international de Winnipeg – automne 2004
- Aéroport international Trudeau, à Montréal – printemps 2005
- Aéroport international Macdonald-Cartier, à Ottawa – printemps 2005

« Notre programme a eu beaucoup de succès jusqu'à maintenant », dit M^me^ Dimasuay, « et nous entendons en tirer tous les avantages possibles. Par ailleurs, nous sommes tous conscients que la technologie biométrique est d'abord et avant tout un outil. Ce n'est qu'un élément d'un processus de sécurité plus vaste ».

NUMÉRO SPÉCIAL SUR LA BIOMÉTRIE

RASSEMBLER les pièces du casse-tête

POUR RENDRE POSSIBLE L'IDENTIFICATION EN TEMPS RÉEL

LE SERGENT C.H. CARL MCDIARMID, DE LA GRC (À GAUCHE), ET LLOYD BUNBURY, CHEF DU PROJET D'IDENTIFICATION EN TEMPS RÉEL DE LA GRC, DEVANT UN LECTEUR BIOMÉTRIQUE LIVESCAN

C'EST EN 2000 QUE LE PROJET D'IDENTIFICATION EN TEMPS RÉEL A ÉTÉ INCORPORÉ DANS L'INITIATIVE DU RÉSEAU CANADIEN D'INFORMATION POUR LA SÉCURITÉ PUBLIQUE (RCISP) LANCÉE PAR LE GOUVERNEMENT DU CANADA. L'OBJECTIF DE CE PROJET EST DE SIMPLIFIER ET D'ACCÉLÉRER LES SERVICES D'INFORMATION ET D'IDENTIFICATION DE LA GRC ET DE FACILITER LA COMMUNICATION DE RENSEIGNEMENTS À L'ÉCHELLE INTERNATIONALE — TOUT PARTICULIÈREMENT EN CE QUI CONCERNE L'IDENTIFICATION DES EMPREINTES DIGITALES, LES VÉRIFICATIONS D'ANTÉCÉDENTS CRIMINELS ET LE MAINTIEN D'UNE BASE DE DONNÉES NATIONALE SUR LES CASIERS JUDICIAIRES.

À CE JOUR, PLUS DE TROIS MILLIONS DE FICHIERS D'EMPREINTES DIGITALES ONT ÉTÉ TRANSPOSÉS EN FORMAT ÉLECTRONIQUE NORMALISÉ À HAUTE RÉSOLUTION AFIN QUE LE SYSTÈME PUISSE LES UTILISER; 144 LECTEURS BIOMÉTRIQUES LIVESCAN ONT ÉTÉ INSTALLÉS PARTOUT AU CANADA; ET UNE ANALYSE APPROFONDIE DE RENTABILISATION DE CES APPAREILS A ÉTÉ PRÉSENTÉE AUX CADRES DIRIGEANTS DE LA GRC.

La prochaine étape, selon Lloyd Bunbury, gestionnaire du projet d'identification en temps réel de la GRC, consiste à rassembler les pièces du casse-tête.

« Il s'agit d'une tâche énorme », dit M. Bunbury. « Mais le résultat final en vaut la peine. Il est question de réduire de quelques semaines à seulement quelques heures le temps nécessaire pour vérifier l'identité et les casiers judiciaires. Et les avantages qu'en retireront les services de police du Canada seront inestimables. »

Les buts du projet d'identification en temps réel sont les suivants : retourner, en moins de deux heures, les identités judiciaires transmises numériquement; mettre tous les casiers judiciaires à jour en moins de 24 heures; et traiter les habilitations de sécurité civiles en moins de 72 heures. Les avantages de tels délais d'exécution sont évidents lorsqu'on prend conscience du retard actuel dans le traitement des demandes de renseignements —et du nombre de nouveaux dossiers qui attendent d'être saisis dans le système de fichiers existant.

« Il faudrait plus de neuf mois pour rattraper le retard [dans les transactions touchant les empreintes digitales et les casiers judiciaires], à condition de ne recevoir aucune demande de mise à jour », dit M. Bunbury. « Sans le RCISP, cet arriéré représente de l'information dont les services policiers peuvent avoir besoin dès aujourd'hui et qui ne peut être mise en commun. »

L'IMPORTANCE DE LA PLANIFICATION

L'analyse de rentabilisation du RCISP décrit plus de 3 000 exigences opérationnelles et techniques du système qui remplacera éventuellement le Système informatisé de dactyloscopie, le Système d'inscription, de mise à jour et de contrôle des casiers judiciaires, le Système de documents actifs (ADS) et le Fichier judiciaire nominatif. Toutes ces exigences ont été étudiées par les principales parties intéressées — y compris les utilisateurs du système et les fournisseurs qui devront élaborer celui-ci.

« Pour gérer un projet de cette envergure », dit M. Bunbury, « une base de données nationale qui sera alimentée et utilisée par des milliers d'organisme de justice et d'application de la loi, vous devez être incroyablement minutieux dans vos préparatifs. En sollicitant la participation des fournisseurs dès le départ, nous avons pu nous assurer que nos exigences n'étaient pas irréalistes, irréalisables ou biaisées en faveur de l'expertise d'une société en particulier. »

UN SYSTÈME BIOMÉTRIQUE MULTIMODAL

À l'heure actuelle, les empreintes digitales sont le principal identificateur biométrique stocké dans le système d'identification en temps réel, mais ce système est en mesure de traiter un plus large éventail de données, notamment les empreintes des paumes et les photos servant à la reconnaissance faciale.

Déjà engagée dans un projet distinct mais connexe, la GRC a mis en service le SARSAID (Système d'accès régional au Système automatisé d'identification dactyloscopique) dans 90 endroits différents au Canada; les services policiers disposent ainsi de la technologie nécessaire pour consigner et consulter électroniquement, à raison de 1 000 pixels au pouce, des renseignements sur les scènes de crimes. Ces renseignements seront éventuellement déposés eux aussi dans le système d'identification en temps réel.

« Nous allons procéder par étape », dit M. Bunbury. « Au début, la recherche ne pourra porter que sur les empreintes digitales. Mais au fil du temps, nous pourrons accroître l'information disponible afin d'englober les empreintes des paumes et les visages. »

Comme les données proviennent de sources multiples — et sont accessibles à de nombreux organismes — l'équipe du projet d'identification en temps réel accorde énormément d'importance aux normes, en particulier au document de contrôle d'interface des Services nationaux de police (SNP) et du National Institute of Standards and Technology (NIST), lequel régit l'échange de renseignements biométriques.

« Ce document de contrôle d'interface est une variante de la norme ANSI-NIST (American National Standards Institute et National Institute of Standards and Technology) qui a été élaborée par et pour les services policiers », dit M. Bunbury. « Il tient compte des besoins de la GRC, du FBI, d'Interpol et d'autres organismes. Nous savons que l'Organisation internationale de normalisation est en train d'élaborer ses propres normes biométriques, et nous avons participé activement à sa démarche parce que nous voulons nous assurer que le travail que nous avons effectué à ce jour est protégé sur la scène internationale. Beaucoup de temps et d'énergie ont été consacrés à l'établissement d'un consensus et d'une infrastructure. »

PERSPECTIVES

Le déploiement d'appareils LiveScan en 2001-2002 — et la création d'une interface de réseau — ont permis à la GRC de commencer à traiter électroniquement les demandes urgentes d'identification en temps réel, même si l'élaboration du système officiel d'identification en temps réel n'est pas encore terminée.

« Les gens se demandaient pourquoi nous installions les appareils LiveScan avant de disposer d'une base de données modernisée pour les alimenter », reconnaît M. Bunbury. « Nous avons estimé que c'était une bonne chose de mettre les outils entre les mains des utilisateurs et de leur donner l'occasion de se familiariser avec ceux-ci à l'échelon local, de façon à ce qu'ils puissent les incorporer dans leurs processus de déroulement des opérations. Aux États-Unis, où les autorités ont établi un système semblable au système d'identification en temps réel, on a commencé par mettre en place l'infrastructure et on a ensuite dû attendre que les utilisateurs soient prêts à s'en servir. En réalité, même si cela est peut-être souhaitable, il est impossible de faire les deux en même temps. »

M. Bunbury est donc désireux de présenter une demande de propositions aux fournisseurs de technologie et de passer à l'étape de la conception et de l'élaboration du projet. Il s'attend à ce que la demande de propositions soit présentée au cours de l'automne 2004.

« Le gros défi qui nous attend », dit-il, « c'est la complexité du système. En décrivant nos 3 000 exigences opérationnelles, nous avons pris grand soin de dire aux fournisseurs *quels* étaient nos besoins, mais nous avons également évité de leur suggérer des *façons* de satisfaire ces besoins. Ce sont les experts qui doivent nous proposer des moyens; nous voulons qu'ils nous fassent bénéficier de leurs pratiques exemplaires. »

En raison de la complexité du projet, la GRC a insisté pour participer au jour le jour au processus de conception, en travaillant directement avec les concepteurs à l'élaboration du produit final. « Nous voulons vraiment que ce système soit adapté aux besoins de tous les organismes d'application de la loi », dit M. Bunbury. « C'est un système qui peut devenir un élément clé pour assurer la sécurité publique — surtout parce que les données biométriques sont de plus en plus importantes dans le travail de police et de protection de la sécurité publique. »

Le déploiement d'appareils LiveScan en 2001-2002 — et la création d'une interface de réseau — a permis à la GRC de commencer à traiter électroniquement les demandes urgentes d'identification en temps réel, même si la mise au point du système officiel d'identification en temps réel n'est pas encore terminée.

COUP D'ŒIL SUR LES EFFORTS CONSTANTS QUE DÉPLOIENT LES PARTENAIRES DU RÉSEAU CANADIEN D'INFORMATION POUR LA SÉCURITÉ PUBLIQUE POUR COLLABORER ET SE COMMUNIQUER DES RENSEIGNEMENTS

PROFILS DE PARTENAIRES

Jim Chu, chef adjoint des services de soutien du Service de police de Vancouver

Portail d'information policière et collaboration

Grâce à une attitude « axée sur l'action », l'IIJ progresse rapidement en Ontario et en Colombie-Britannique

En février 2003, Brian Collins — alors chef du Service de police de London — a fait parvenir à ses collègues de Windsor, Toronto, Ottawa et d'autres villes ontariennes une lettre dans laquelle il exprimait le désir de faire quelque chose pour corriger les lacunes de la communication de renseignements entre les Services de police de la province. « Je trouvais la situation scandaleuse », dit M. Collins. « J'étais conscient de toute l'information qui pouvait être mise en commun — qui *aurait dû* l'être automatiquement — et je savais qu'il était facile de le faire. Dans ma lettre, je disais essentiellement que le moment était venu d'agir en ce domaine. »

Et c'est ce que mes collègues ont fait. Le 16 avril dernier, des représentants de différents services de police de l'Ontario se sont réunis à London et ont établi un plan pour échanger de l'information. Une équipe de mise en œuvre de ce plan a été constituée sur-le-champ; cette équipe était dirigée par Eldon Amoroso et Rick Gillespie. (M. Amoroso est directeur principal du département de la technologie de l'information au Service de police de London; M. Gillespie est directeur de la Division des enquêtes criminelles.)

Le 17 septembre 2003, London et Windsor étaient en mesure de se transmettre des renseignements par l'entremise d'un portail d'information policière (Law Enforcement Information Portal - LEIP). Le 6 novembre, Ottawa était également en ligne. Et Toronto — le plus gros service de police municipal au Canada — a commencé à fournir des données à compter du 31 mars 2004.

Ces résultats sont assez impressionnants après un peu plus d'un an de travail — et seulement trois rencontres formelles de l'équipe de projet. Et ils sont extrêmement gratifiants pour M. Collins qui a pris sa retraite en mars 2004, après 34 années de service.

« Les résultats que nous avons obtenus jusqu'à maintenant sont la preuve qu'une telle démarche ne tient pas du mystère — et ne doit pas nécessairement devenir un cauchemar bureaucratique. Il suffit que la haute direction s'engage dans le projet et se fixe un seul but réaliste à la fois », ajoute M. Collins.

L'AVANTAGE DE L'EXPÉRIENCE

Il est également utile de solliciter le point de vue d'une personne d'expérience — qui connaît les pièges possibles et la manière de les éviter. Pour l'équipe du projet de portail d'information policière de l'Ontario, cette personne était Jim Chu, chef adjoint des services de soutien du Service de police de Vancouver. M. Chu est l'un des instigateurs d'un portail semblable créé en Colombie-Britannique, lequel est en service depuis septembre 2002. Aujourd'hui, dans cette province, tous les services de police municipaux et détachements de la GRC ont accès au portail d'information policière.

En Colombie-Britannique, c'est la création de PRIME, l'Environnement de gestion de l'information sur les dossiers de la police, qui est à l'origine du portail d'information policière. Le but de PRIME était de doter tous les services de police de la Colombie-Britannique d'un système commun et normalisé de gestion des dossiers (SGD) — un projet d'une envergure colossale. Entre-temps, c'est le portail d'information policière qui permet la communication de renseignements entre les différentes installations du SGD. Lorsqu'ils seront tous reliés à PRIME, les postes de police de la Colombie-Britannique utiliseront ce portail pour échanger de l'information avec des organismes extérieurs.

« On en apprend beaucoup lorsqu'on conçoit, met à l'essai et déploie sa propre application », dit M. Chu. « Pas seulement sur le plan technique, mais aussi sur les aspects qui concernent la gestion et la logistique de mise en œuvre du projet. C'est avec grand plaisir que j'ai fait part à l'équipe de l'Ontario de ce que nous avions découvert dans le cadre de notre expérience. Lorsqu'on parle de communiquer l'information de la justice, il n'y absolument aucune raison de réinventer la roue. »

M. Chu a remis à l'équipe du portail de l'information policière de l'Ontario le protocole d'entente sur l'échange de renseignements, élaboré par la Colombie-Britannique, ainsi que les résultats d'une recherche sur les conséquences de la création d'un système électronique — sur le plan juridique et sur celui de l'accès à l'information. « Nous savions que l'Ontario devrait adapter ce matériel à ses propres besoins », dit M. Chu, « mais les membres de l'équipe ontarienne disposaient tout au moins d'éléments de départ. Nous les avons également aidés à satisfaire aux exigences en matière de sécurité pour leur architecture et leur réseau. Nous avions longuement discuté de ces aspects avec les responsables de la sécurité à la GRC et nous avions déjà franchi beaucoup d'obstacles. Le groupe de l'Ontario a profité de notre expérience. »

LE MONTRER PLUTÔT QUE LE DIRE

M. Chu explique que l'équipe de la Colombie-Britannique avait compris, pour ainsi dire dès le départ, que la meilleure façon de faire largement « accepter » le portail d'information policière était de le mettre sur pied — à la plus grande échelle possible — et d'en montrer les avantages sur le terrain. L'équipe de projet a donc recruté des services de police qu'elle a reliés au portail d'information policière, sans les obliger à y faire des contributions.

« Pour mettre un projet en œuvre de cette façon », fait remarquer M. Chu, « vous devez obtenir un excellent rapport coût-efficacité ». « Nous n'avons pas engagé de conseillers à honoraires élevés », dit-il. « Des services de police nous ont fourni du personnel pour le projet —qui a nécessité des centaines, voire des milliers d'heures de ressources humaines. C'est ainsi que vous devez procéder. Et nous avions l'appui du Secrétariat de l'intégration de l'information de la justice, un appui dont nous sommes très reconnaissants. »

Dès que l'utilité du système est devenue manifeste, les utilisateurs ont montré de plus en plus d'empressement à y faire eux aussi une contribution en retour, explique M. Chu.

« Les gens se sont branchés et ont vu ce qu'ils pouvaient retirer du système — ils *voulaient* y contribuer. Et lorsqu'ils ont constaté à quel point le portail d'information policière était performant, les décideurs de haut niveau ont reconnu qu'il fallait le maintenir en service; et c'est exactement la décision qu'ils ont prise. »

OUVERTURE

En Ontario, il n'y a pas eu de mouvement provincial en faveur de la création d'un système commun de gestion des dossiers, comme cela a été le cas en Colombie-Britannique. On a donc dû concevoir le portail d'information policière de l'Ontario au vu et au su de tous, en veillant à ce tous les SGD puissent s'y connecter.

« Nous avons déjà fait la preuve que nous pouvons répondre aux besoins de différents systèmes », dit le directeur principal Eldon Amoroso. « London, Windsor et Ottawa utilisent toutes la même marque de SGD, mais Toronto possède un système maison, et nous avons

« Des services de police nous ont fourni du personnel pour le projet — qui a nécessité des centaines, voire des milliers d'heures de ressources humaines. C'est ainsi que vous devez procéder. »

LE MODE DE FONCTIONNEMENT DU PORTAIL D'INFORMATION POLICIÈRE

En Ontario, les services de police reliés au système du portail d'information policière continuent de télécharger vers l'amont des renseignements sur les incidents, dans leurs propres systèmes de gestion des dossiers. Tous les membres des services de police reliés au système peuvent utiliser le portail d'information policière pour chercher des renseignements de base concernant des personnes et des véhicules. Ce genre de recherche génère un rapport sous forme d'index concernant des renseignements de niveau élevé. Selon l'autorisation qui leur a été accordée, les membres peuvent ensuite accéder en mode descendant au SGD afin d'obtenir des renseignements plus détaillés.

De gauche à droite dans la photo : Brian Collins (chef retraité), Eldon Amoroso (directeur principal), Case Huysmans (analyste principal des systèmes), Richard Gillespie (directeur)

Photo reproduite avec l'aimable autorisation du Service de police de London

commencé à télécharger ses données de production en mars. »

Étant donné que l'interopérabilité du portail d'information policière de l'Ontario a été démontrée, M. Amoroso ne voit pas pourquoi ce système municipal ne pourrait pas se raccorder à différents autres systèmes — allant du système partagé de gestion des dossiers du groupe OPTIC (constitué de 40 services de police municipaux et de la Police provinciale de l'Ontario) au portail d'information policière de la Colombie-Britannique.

Étant donné que de multiples systèmes de gestion des dossiers étaient en cause dans le système de l'Ontario, il était très important d'établir une norme de données pour l'interface. À titre d'exemple, ce qu'un système classe comme « sujet », peut être classé comme « suspect » par un autre système.

« Nous avons demandé à un analyste des systèmes de gestion de rencontrer des représentants de tous les services concernés afin d'examiner ces questions et d'élaborer une norme de travail pour le système du portail d'information policière », dit M. Amoroso. « Tous les services de police continuent de saisir des données dans leur propre SGD à leur façon, mais ils doivent utiliser une terminologie normalisée pour interroger le portail d'information policière ou examiner les résultats d'une recherche. »

M. Amoroso affirme que la norme de données du portail d'information policière est très proche de la norme de données du RCISP et qu'il ne sera pas très difficile de concilier les deux.

PREMIERS RÉSULTATS

Le détective en chef Rick Gillespie affirme que les utilisateurs du portail d'information policière de l'Ontario ont déjà commencé à constater les avantages concrets du système. Il cite l'exemple d'un cas de violence familiale. Le Service de police de London ne savait pas qu'un individu accusé de violence familiale avait déjà été accusé d'une infraction semblable à Windsor. C'est en effectuant une recherche dans le portail d'information policière que l'agent d'enquête a découvert les antécédents de cette personne — et ainsi obtenu des renseignements supplémentaires pour « justifier » la demande d'enquête sur le cautionnement. Sans le portail d'information policière, ces éléments cruciaux des antécédents criminels de l'accusé n'auraient pas été révélés.

« Cet exemple montre également l'importance de ce portail pour décloisonner l'information », dit M. Gillespie. « Windsor est juste au sud de London, mais sans le portail d'information policière, ces renseignements n'auraient pas été mis en commun. »

Jim Chu affirme que l'expérience vécue en Colombie-Britannique est semblable. « D'un côté du chemin Boundary, à Vancouver, ce sont les policiers de Vancouver qui patrouillent; de l'autre côté, c'est la GRC. Les escrocs profitent de l'incapacité des Services de police de s'échanger des renseignements. »

CONSOLIDER LE SYSTÈME

Eldon Amoroso affirme que lui-même et ses collègues responsables du portail d'information policière de l'Ontario ont reçu des demandes de nombreux autres services de police qui voulaient se brancher au portail. « Le portail suscite actuellement beaucoup d'intérêt, et c'est exactement ce que nous voulons. À vrai dire, la technologie actuelle nous permettrait de brancher toute la province de l'Ontario au portail en moins d'un an. »

L'Ontario continue d'ajouter des membres au réseau de son portail d'information policière, tandis que la Colombie-Britannique explore de nouvelles orientations.

« En ce moment-même à Victoria », dit Jim Chu, « nous sommes en train de rendre le portail d'information policière accessible aux agents sur le terrain, par l'intermédiaire du réseau sans fil. Les agents qui patrouillent dans les rues auront donc accès à de l'information en temps réel en provenance de Vancouver. Et le Service de police de Vancouver a commencé à échanger des renseignements avec le détachement de la GRC de Richmond. C'est un progrès considérable pour nous. Je ne connais pas d'autre endroit au Canada où un organisme non relié au Système de récupération de renseignements judiciaires (SRRJ)[5] peut obtenir des renseignements de la GRC sur son ordinateur portatif alors qu'il se trouve sur le terrain. »

PHOTO REPRODUITE AVEC L'AIMABLE AUTORISATION DU SERVICE DE POLICE DE VANCOUVER

Et, comme nous l'avons déjà mentionné, le portail d'information policière de la Colombie-Britannique sert de pont pour accéder au système provincial normalisé de gestion des dossiers PRIME. Des travaux sont en cours pour faire passer PRIME d'un réseau de bases de données discrètes à une seule base de données massive virtuelle. Pourquoi avoir pris une telle décision alors que le portail d'information policière permet déjà aux différents services de consulter leurs SGD respectifs?

« Pour le rendre encore plus accessible », répond simplement M. Chu. « L'objectif est d'obtenir davantage de renseignements plus rapidement. Le portail d'information policière donne accès à environ 90 % des renseignements contenus dans les SGD des différents Services de police. Le mode de consultation du portail est le même pour tous. Mais le portail ne peut pas tout faire. La solution réside dans un seul SGD multijuridictionnel. Mais ce genre de SGD n'est pas encore réalité – et il y a déjà longtemps que nous en avons besoin. »

La région de la capitale Victoria — qui comprend quatre services de police municipaux — est déjà reliée au nouveau système multijuridictionnel PRIME, ce qui englobe toute l'interface du portail d'information policière. Les Services de police de Vancouver et les autres services de police du Lower Mainland, en Colombie-Britannique, doivent également passer plus tard ce printemps de leurs bases de données autonomes au système multijuridictionnel PRIME.

RÉFLEXION SUR LA RÉUSSITE

Brian Collins, Eldon Amoroso et Rick Gillespie sont tous d'accord pour dire que différents facteurs ont contribué au succès initial du projet de portail d'information policière de l'Ontario. Le commissaire Zaccardelli de la GRC s'est engagé à soutenir le projet — et la GRC a fourni l'infrastructure de la connectivité par l'entremise de son Réseau des services nationaux de police. Ces appuis ont accéléré la mise en œuvre du portail. Et les coûts de démarrage ont été en partie couverts par deux subventions du Comité consultatif du programme du service de l'aide technique (CCPSAT) de Statistique Canada.

Mais le facteur déterminant le plus important, et de loin, était la volonté de faire quelque chose.

« Nous avons créé un serveur, nous avons établi des connexions, notre croissance est partie de là », dit M. Collins. « Dès le départ, nous nous sommes assurés que les premières rencontres de l'équipe ne serviraient pas à discuter des problèmes, mais bien à prendre des décisions pour que le travail nécessaire soit accompli. Nous savions que ce ne serait pas parfait d'emblée; nous savions que nous ne pouvions bâtir tout le système d'un coup. Mais nous étions déterminés à faire *quelque chose* dans le domaine du crime mondialisé. Le portail d'information policière fait réellement partie de notre vision philosophique plus générale, une conscience de plus en plus grande du fait que les services de police intégrés sont absolument indispensables à la sécurité publique au XXIe siècle. »

[5] Le Système de récupération de renseignements judiciaires (SRRJ) est le système en place à la GRC. Un nouveau système, le Système d'incidents et de rapports de police (SIRP), est en cours de déploiement dans de nombreuses régions du pays, mais pour l'instant, les détachements de la GRC stationnés à Richmond et ailleurs en Colombie-Britannique demeurent des utilisateurs du SRRJ.

L'engagement des dirigeants

Les chefs de police suivants ont demandé à leurs organisations d'appuyer la phase 1 du portail d'information policière de l'Ontario :

- chef Brian Collins, Service de police de London
- chef Glen Stannard, Service de police de Windsor
- chef Vince Bevan, Service de police d'Ottawa
- chef Julian Fantino, Service de police de Toronto

Des partenaires du Québec et de la Saskatchewan

SE BRANCHENT AU SYSTÈME DE GESTION DES DÉLINQUANTS DU SERVICE CORRECTIONNEL DU CANADA

Les efforts déployés par les partenaires de la justice pénale au Canada pour renouveler les systèmes de gestion des cas ne visent pas seulement à trouver de nouvelles façons d'offrir des services à la clientèle existante — l'amélioration de la connectivité chez les homologues de l'extérieur est tout aussi importante. Il suffit pour s'en convaincre de jeter un coup d'œil sur les réalisations de l'équipe du Projet de renouvellement du Système de gestion des délinquants (SGD), du Service correctionnel du Canada. Depuis le début de 2001, cette équipe a réussi à apporter d'importantes améliorations au SGD, lequel sert à recueillir, stocker et récupérer des renseignements sur les délinquants placés sous la responsabilité du système correctionnel fédéral canadien.

« La mise en commun de l'information est une priorité essentielle du Projet de renouvellement du SGD depuis le tout début », explique George Pinatel (gestionnaire de la mise en commun de l'information et des communications dans le cadre du Projet de renouvellement du SGD). « C'est quelque chose dont nous sommes particulièrement fiers car, jusqu'à maintenant, nous sommes la seule organisation membre du Réseau canadien d'information pour la sécurité publique à avoir réussi à échanger des renseignements avec des organisations de l'extérieur. »

D'ici 2005, plus de 2 000 nouveaux utilisateurs de l'extérieur auront été branchés au système renouvelé, ce qui rendra possibles des échanges de données contrôlés, sécurisés et limités, conformément à l'accès à l'information permis par la loi. Partout au Canada, les services de police ont accès au SGD depuis 2003 (voir à ce sujet le nº 3 d'*IIJ@l'œuvre*), mais les organismes correctionnels provinciaux et territoriaux ont également obtenu la connectivité avec le système correctionnel du Canada. Les premières ententes à cet effet ont été conclues avec le Québec et la Saskatchewan (une entente distincte touchant la prestation de services, de portée et d'application différentes, a également été conclue avec le Territoire du Yukon).

Grâce aux protocoles d'entente conclus avec les deux provinces, les autorités correctionnelles du Québec et de la Saskatchewan bénéficient maintenant d'une meilleure connectivité avec le Service correctionnel du Canada (SCC). Ces deux provinces ont accès 24 heures sur 24 à un menu spécial de l'interface du SGD, conçu spécialement pour répondre à leurs besoins par l'équipe du Projet de renouvellement du SGD.

Les ententes conclues avec le Québec et la Saskatchewan se sont traduites par un tout nouvel échange électronique d'information, grâce auquel les deux provinces ont

Photo reproduite avec l'aimable autorisation du Service correctionnel du Canada

maintenant accès à une foule de renseignements sur les délinquants et délinquantes dont ils ont la garde.

« Ces ententes procurent à nos homologues provinciaux un accès pour simple lecture aux dossiers du SGD sur certains délinquants, selon le principe du besoin de connaître », explique M. Pinatel. « Cet accès leur est accordé lorsqu'ils ont sous leur garde une personne qui a déjà fait partie des délinquants ou délinquantes sous responsabilité fédérale. » Ces ententes comportent également une clause de réciprocité en vertu de laquelle le SCC a accès au système provincial et territorial de gestion des délinquants, dans le cas de délinquants dont il a déjà eu la garde par le passé.

Afin de respecter la législation relative à la protection de la vie privée ainsi que la *Loi sur le système correctionnel et la mise en liberté sous condition*, il est essentiel d'établir des contrôles de l'échange de renseignements. Il n'en demeure pas moins que le niveau de connectivité que permettent ces ententes est essentiel à la sécurité publique. Les décisions prises dans le système correctionnel peuvent avoir une incidence directe sur la sécurité des citoyens et citoyennes. Le moindre petit renseignement supplémentaire sur un délinquant, qui peut être communiqué et ajouté au dossier du cas, peut changer bien des choses. Par exemple, M. Pinatel cite les conclusions d'une enquête menée au Québec, en 2002, concernant la mort d'un garçon de 13 ans assassiné en 2000 par un délinquant qui avait été mis en liberté sous condition par les autorités correctionnelles provinciales. Les auteurs du rapport d'enquête recommandaient notamment d'améliorer la communication de renseignements entre la Commission québécoise des libérations conditionnelles et ses homologues fédéraux. Une telle amélioration permettra aux autorités provinciales de savoir immédiatement si le délinquant dont elles examinent le dossier a déjà purgé une peine dans un établissement correctionnel fédéral pour une infraction à une loi fédérale. Grâce à l'accord de réciprocité, les autorités fédérales jouissent du même accès à l'information provinciale.

Le raccordement du Québec et de la Saskatchewan au SGD (ainsi que l'entente distincte conclue avec le Territoire du Yukon) n'était que le début des activités de communication de renseignements entreprises par l'équipe responsable du Projet de renouvellement du SGD. Depuis, d'autres ententes ont été négociées avec la Colombie-Britannique, le Nouveau-Brunswick, Terre-Neuve et le Labrador. La phase de mise en œuvre de ces ententes se terminera avant la fin de 2004.

L'équipe du Projet de renouvellement du SGD a également les yeux tournés vers la prochaine étape, explique M. Pinatel. « Lorsque nous aurons terminé le travail de migration du SGD », dit-il, « nous examinerons les façons de transférer les renseignements sur les délinquants d'un système à l'autre, entre les partenaires fédéraux, provinciaux et territoriaux du système correctionnel du Canada, afin d'éliminer les doubles emplois entre les différentes autorités. » Cette initiative devrait être achevée au cours des deux prochaines années.

PROFILS DE PARTENAIRES

Les points de vue du Québec et de la Saskatchewan sur la connectivité au SGD

Afin de connaître les points de vue du Québec et de la Saskatchewan — les deux provinces entièrement raccordées au SGD — *IIJ@L'ŒUVRE* a interviewé des fonctionnaires provinciaux responsables de la gestion et de l'administration de ces projets dans leurs domaines respectifs : Pierre Bérubé (analyste de systèmes, Services correctionnels du Québec, ministère de la Sécurité publique) et George Clark (gestionnaire des systèmes d'information, ministère des Services correctionnels et de la Sécurité publique de la Saskatchewan — Division des services correctionnels pour adultes).

IJI@l'Œuvre : Quelles sont les principaux défis que vous avez dû relever lors de la mise en œuvre de la connectivité avec le SGD, à la suite de la conclusion d'un protocole d'entente avec le Service correctionnel du Canada

M. Bérubé (Québec) : Pour nous, l'un des principaux défis consistait à élaborer tous les protocoles nécessaires d'échange d'information au sein de notre organisation. Afin de respecter les termes du protocole d'entente, nous devions instaurer des façons de procéder communes, conformément aux exigences du Service correctionnel du Canada en matière de sécurité. Une fois cette étape franchie, nous avons pu nous attaquer à l'aspect technique, consistant entre autres à mettre nos systèmes à l'essai pour assurer une connectivité sécurisée et conforme aux normes établies.

M. Clark (Saskatchewan) : L'une de nos principales tâches consistait à définir les conditions dans lesquelles des renseignements pouvaient être échangés. Une fois cet objectif atteint, nous devions déterminer la façon dont les membres du personnel devaient procéder pour demander des renseignements, et établir des structures pour la distribution et le stockage de l'information.

IJI@l'Œuvre : Sur le plan pratique, quels sont les avantages que votre province retire de cette entente sur la communication de renseignements?

M. Bérubé (Québec) : Le travail nécessaire pour respecter les termes du protocole d'entente conclu avec le SCC a été très exigeant. Ce n'était pas facile — il nous a fallu environ six mois pour achever cette tâche — mais nous pensons que cette étape a été profitable. Nous avons dû examiner attentivement nos façons de procéder et les mesures à prendre pour réussir à échanger des renseignements à l'intérieur de notre système de documents sur les délinquants. Il faut rappeler, compte tenu de la nature du système correctionnel, à quel point il est difficile d'être précis en ce qui concerne les avantages de la communication de renseignements. Nous profitons tous les jours de l'amélioration de l'échange de renseignements issue de l'entente, mais ces avantages devraient être transparents. Ils devraient se fondre en douceur dans les systèmes qui sont déjà en place à l'intérieur du système correctionnel québécois. On pourrait dire « pas de nouvelles, bonnes nouvelles » lorsqu'il est question de la communication de renseignements sur les délinquants.

M. Clark (Saskatchewan) : Ce projet a coïncidé avec l'adoption d'une grande orientation de principe concernant la gestion des cas dans les services correctionnels pour adultes en Saskatchewan. Notre approche consistait à élaborer un plan de gestion du cas pour chaque délinquant et à communiquer les détails de ce plan aux agents concernés de gestion des cas. Cette démarche a débouché sur la mise en œuvre en ligne d'évaluations du risque, de plans correctionnels et de suivis des plans correctionnels, y compris des mises à jour spéciales concernant la participation du délinquant à des programmes tels que le Programme de prévention de la toxicomanie chez les délinquants. La capacité d'examiner le vécu des délinquants en collaboration avec nos homologues fédéraux nous a permis de prendre de meilleures décisions, tant au chapitre de l'évaluation du risque et des besoins que des stratégies d'intervention adaptées à chacun des cas.

IJI@l'Œuvre : Êtes-vous satisfaits des résultats du protocole d'entente

M. Bérubé (Québec) : Oui. Pour nous, ce projet a été très encourageant. Il a montré que nous pouvions travailler ensemble à trouver des solutions aux questions qui préoccupent nos citoyens, telles que la sécurité publique. Nous sommes spécialement contents des apprentissages que cet exercice a rendu possibles : grâce à cette expérience, nous sommes aujourd'hui une organisation plus intelligente.

M. Clark (Saskatchewan) : Le protocole est important pour nous. Il établit les fondements et les paramètres généraux de la communication des renseignements. Au fur et à mesure que le projet progressait, nous avons dû veiller à bien expliquer le protocole d'entente et toute la législation pertinente à nos utilisateurs. Cette discussion continue d'évoluer, car le personnel change et, devant des situations nouvelles, certains ressentent le besoin de mettre leurs connaissances à jour.

Michael Boudreau (à gauche), directeur des programmes et de la planification à la Division des services communautaires et correctionnels du ministère de la Sécurité publique, au Nouveau-Brunswick, et Robert Cyr, directeur du programme PIMITS au ministère de la Sécurité publique du Nouveau-Brunswick

MISE EN ŒUVRE

Le Nouveau-Brunswick fait des pas de géant dans le domaine de l'IIJ

Plusieurs éléments essentiels expliquent la réussite de l'intégration de l'information de la justice (IIJ). La technologie est manifestement l'un de ces éléments : disposer des outils nécessaires pour répondre aux exigences opérationnelles. Le programme d'action en est un autre : mettre en place les structures permettant une communication efficace de l'information.

La gestion de projet est un troisième élément. Et c'est grâce à leur gestion intelligente des projets que les organismes de justice pénale du Nouveau-Brunswick ont réussi, ces dernières années, à aller de l'avant avec deux importantes initiatives de communication de l'information : un Programme de gestion de l'information policière et du partage des technologies de l'information (le programme PIMITS) ainsi qu'un Système d'information sur la clientèle (SIC), à la Division des services communautaires et correctionnels du ministère de la Sécurité publique de la province.

UNE SAGESSE DUREMENT ACQUISE

Michael Boudreau est directeur des programmes et de la planification à la Division des services communautaires et correctionnels du ministère de la Sécurité publique, au Nouveau-Brunswick — et chef du projet du SIC en cours. Il affirme que l'intérêt de la province pour les systèmes d'intégration de l'information de la justice remonte au début des années 1990. « À l'époque, un projet d'envergure appelé Justice intégrée Nouveau-Brunswick (JINB) avait été lancé. » Selon M. Boudreau, il s'agissait d'un projet extrêmement ambitieux : un projet global de conception descendante, qui visait à relier électroniquement tous les systèmes de justice de la province. « En fin de compte, ce projet s'est révélé impossible à réaliser. C'était un projet de trop grande envergure et trop coûteux, et ce fut un échec. Mais nous avons tiré de précieuses leçons de cette expérience. En particulier que vous ne devez pas vous attendre à atteindre tous vos objectifs en même temps lorsque vous entreprenez des projets de ce genre. »

L'échec essuyé a également fait comprendre aux responsables du projet à l'époque que, quelle que soit l'importance des aspects technologiques, les projets d'IIJ ne reposent pas uniquement sur la technologie de l'information. Pour être efficace, le système mis en place doit répondre aux besoins fonctionnels des utilisateurs sur le terrain.

« Nous avons demandé à certains de nos meilleurs employés de se consacrer

exclusivement au processus de conception et de mise au point du système », dit M. Boudreau. « Bien entendu, il y a un coût associé à ce genre de décision — un coût en ressources humaines. Mais nous n'aurions certainement pas pu procéder autrement. »

LA BONNE SOLUTION

Le Système d'information sur la clientèle (SIC) a été mis en service en 1999 et achevé en 2002. Installé à 70 endroits différents dans l'ensemble du Nouveau-Brunswick, ce système englobe la phase *des dispositions* du processus judiciaire — c'est–à-dire la phase au cours de laquelle les peines sont calculées et appliquées. Entièrement sécurisé, le SIC contient des renseignements sur les adultes et les jeunes contrevenants dans les établissements et dans les centres correctionnels communautaires. Il contient également de l'information sur les victimes.

Le SIC a été conçu pour se raccorder aux systèmes du ministère de la Justice et du ministère de la Famille et des Services communautaires, ainsi qu'au Système de gestion des délinquants (SGD) du gouvernement fédéral. (En fait, pour s'assurer de l'existence d'une interface avec le SGD fédéral, l'équipe responsable du SIC a fait appel à un spécialiste en technologie de l'information du Service correctionnel du Canada).

Élaboré conformément aux normes de données du gouvernement fédéral, le SIC fait actuellement l'objet de modifications visant à le rendre en mesure d'échanger de l'information avec le Centre canadien de la statistique juridique (CCSJ).

Accessible à l'aide d'un navigateur Web sécurisé, le SIC est un système entièrement intégré, doté de la capacité de fournir des renseignements en temps réel sur les délinquants, d'un module complet sur la gestion des cas et d'un dispositif automatisé de calcul des peines — dispositif qui a suscité un grand intérêt chez les autres organisations des services correctionnels.

« Le système que nous avons créé », explique M. Boudreau, « peut communiquer avec d'autres systèmes tout en respectant leur autonomie. L'expérience nous a appris qu'il est tout simplement trop compliqué d'essayer de mettre sur pied un système à partir de zéro. Alors, nous avons conçu un système qui répond à nos besoins ainsi qu'un mécanisme pour le raccorder aux autres systèmes. »

ACCUEIL ENTHOUSIASTE

Selon M. Boudreau, malgré le fait que très peu d'employés de première ligne du ministère possédaient déjà une expérience en informatique, le système électronique SIC a été accueilli avec un grand enthousiasme dans les services correctionnels en établissement ainsi que dans les services correctionnels communautaires.

« Avant l'arrivée du SIC, tous nos dossiers étaient sur support papier », dit M. Boudreau. « Une enquête effectuée auprès des membres du personnel a révélé l'existence d'un niveau élevé d'aisance ou d'aptitude concernant la technologie. Mais presque tout le monde reconnaissait que nos systèmes pouvaient être améliorés. »

Afin de faciliter l'adoption du SIC, le ministère a offert à ses employés une formation poussée en technologie, allant des techniques de base de la saisie au clavier aux camps d'entraînement en informatique, au plein sens du terme. « Je suis convaincu que la formation a été un autre élément clé de notre réussite », dit M. Boudreau. « Les gens ont apprécié le fait que nous ayons pris du temps pour les aider à se sentir à l'aise avec le nouveau système. Ils manifestaient un grand désir d'apprendre. La majorité d'entre eux ont accepté de suivre les cours de formation proposés.

MESURES DE LA RÉUSSITE

Le SIC du Nouveau-Brunswick a suscité beaucoup d'intérêt chez les autres organismes de justice pénale au Canada. Le Secrétariat de l'IIJ, de Sécurité publique et Protection civile Canada, fait la promotion de son modèle de cryptage des données, qu'il souhaite voir devenir le fondement d'une norme nationale. Le Service correctionnel du Canada a fait l'étude d'environ 120 systèmes semblables, un peu partout dans le monde, et classé le SIC parmi les trois meilleurs. Et en 2002, le SIC du Nouveau-Brunswick a remporté le Concours de l'informatique et de la productivité pour l'avenir ainsi qu'un prix KIRA (Knowledge Industry Recognition Award), en plus de se voir décerner une mention spéciale par le premier ministre de la province.

« Nous sommes très fiers de toutes nos réalisations », dit M. Boudreau. « Elles sont le fruit d'un dur travail. L'important est de procéder étape par étape. Même si nous sommes nombreux à souhaiter la mise en place d'un système national commun, celui-ci ne verra pas le jour dans l'immédiat. Mais il y a beaucoup à faire si vous possédez la volonté et la détermination nécessaires. Et progressivement, par petites étapes, les gens constatent rapidement les avantages du système, ce qui leur donne le goût de participer à la démarche. »

TOUS POUR UN

La vision du programme PIMITS est de relier électroniquement tous les Services de police du Nouveau-Brunswick afin d'améliorer leur capacité de créer et d'échanger des renseignements en utilisant des moyens qui réduisent les menaces du crime organisé, des grands criminels et du terrorisme. Ce programme fait partie du plan stratégique du ministère de la Sécurité publique de la province, et son origine remonte au moins aussi loin que le SIC.

Robert Cyr est directeur du programme PIMITS au ministère de la Sécurité publique du Nouveau-Brunswick. Il affirme que les leçons apprises lors de l'élaboration du SIC ont été extrêmement utiles pour propulser le programme PIMITS de l'avant. « Nous réalisons ce projet avec très peu de ressources et nos objectifs sont bien ciblés », ajoute-t-il. « Le bureau responsable du programme se compose de deux personnes, dont moi-même. Nous misons sur l'expertise technique des Services de police municipaux et du ministère de la Sécurité publique du Nouveau-Brunswick. Comme cela a été le cas pour le SIC, nous avons adopté une approche progressive, en nous fixant des jalons réalistes que nous nous efforçons d'atteindre. »

Cette approche a été clairement définie par le comité directeur du programme PIMITS, auquel siègent des membres de haut niveau de tous

les Services de police du Nouveau-Brunswick. M. Cyr cite en exemple la mise en place d'une infrastructure technologique qui facilitera la communication de renseignements dans le cadre du programme PIMITS. Cette infrastructure, qui est un réseau privé, en circuit fermé et sécurisé, comporte déjà des avantages pour les organismes, même si d'autres éléments du système sont encore en cours d'élaboration.

« Avant la mise en place de l'infrastructure, les services de police qui souhaitaient obtenir des renseignements sur certains véhicules automobiles devaient communiquer avec l'ordinateur central de la province auquel ils avaient accès par ligne commutée à faible débit », dit M. Cyr. « Ce procédé était peu commode et coûteux en temps. Aujourd'hui, ils peuvent utiliser l'infrastructure du programme PIMITS et bénéficier d'un accès direct à large bande. »

Parce qu'elle est privée et sécurisée, l'infrastructure du programme répond aux exigences de l'équipe du renouvellement du Centre d'information de la police canadienne (CIPC) en matière de sécurité. Rappelons pour mémoire que deux types de connexion au CIPC sont possibles — une par l'entremise du CIPC pour Windows, et l'autre par l'entremise de l'interface appelée intergiciel asynchrone (MOM – Message-oriented middleware). Le CIPC pour Windows s'applique aux ordinateurs personnels autonomes; l'intergiciel asynchrone est un modèle d'interface pour les ordinateurs personnels *en réseau*, dont la sécurité est une préoccupation importante. Si les responsables du programme PIMITS parvenaient à établir une interface avec le CIPC, les organismes d'application de la loi de l'ensemble du Nouveau-Brunswick en retireraient de grands avantages — car l'interface serait commune à tous. Cette interface commune serait d'une énorme utilité aux plus petits détachements qui n'ont pas les moyens financiers de se procurer la technologie de l'intergiciel asynchrone pour se brancher au CIPC de manière indépendante.

Maintenant que l'infrastructure de réseau est en place, le comité directeur multidisciplinaire a décidé que la prochaine étape consisterait à établir un « bureau central » d'échange d'information.

SE COMMUNIQUER DE L'INFORMATION EN PRÉSERVANT L'AUTONOMIE

Le bureau central du programme PIMITS fera en quelque sorte office de portail. Il permettra aux systèmes locaux de gestion des dossiers (SGD) de se brancher à l'infrastructure partagée du programme PIMITS, tout en laissant à chacun des Services de police la liberté de conserver leurs propres bases de données. Cet aspect est important du point de vue de la convivialité, car il signifie que les agents de première ligne profitent de la nouvelle fonctionnalité sans devoir se familiariser avec un tout nouveau système.

Pour atteindre cette transparence fonctionnelle, l'un des objectifs de conception du programme PIMITS est de convertir les données des SGD d'origine à la norme de données du RCISP, grâce une solution « boîte noire ». En passant par le bureau central, les membres pourront procéder à des recherches et interrogations dans des systèmes autres que leur propre SGD.

Afin de régir l'échange d'information dans le cadre du programme PIMITS, l'équipe responsable de ce projet est en train d'élaborer un protocole d'entente avec le concours du Secrétariat de l'IIJ. La version définitive de ce protocole d'entente exposera la vision du programme PIMITS et décrira les modalités de la communication des renseignements.

REGARD SUR L'AVENIR

Même si elle a opté pour une approche progressive, l'équipe du projet PIMITS fait preuve d'une vision résolument à long terme. « Vous devez penser à l'avenir, même lorsque vous axez vos efforts sur ce que vous pouvez et devez faire immédiatement », dit M. Cyr. « À titre d'exemple, nous avons eu de nombreuses conversations avec l'équipe du renouvellement du CIPC; nous savons que nous allons vouloir nous brancher à ce système et que notre interface devra interopérer avec lui. C'est pourquoi nous avons bâti l'infrastructure qui est actuellement la nôtre — c'est-à-dire une infrastructure sécurisée laquelle répondra à nos exigences en matière de largeur de bande, tout au long de la démarche. »

Comme tout projet d'IIJ, la vision à long terme oblige à poser certaines questions d'ordre financier comme celle-ci : « D'où proviendra le budget pour soutenir le système au fil du temps? » Dans le cas du SIC et du programme PIMITS, la réponse réside, au moins en partie, dans les partenariats entre le secteur public et le secteur privé. En travaillant en étroite collaboration avec des partenaires de l'industrie technologique du secteur privé, les équipes responsables du SIC et du programme PIMITS espèrent que les systèmes qu'ils sont en train d'élaborer seront un jour disponibles sur le marché.

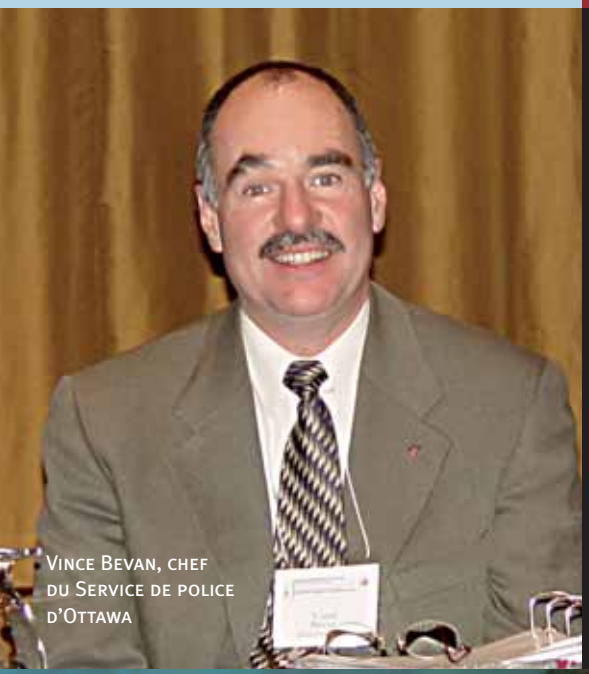
« D'autres administrations sont confrontées aux mêmes difficultés que nous », dit Michael Boudreau. « Elles vont avoir besoin de solutions. L'entente que nous avons conclue avec le partenaire de l'industrie des technologies de l'information qui nous aide dans la conception du SIC, la société xwave, prévoit que cette dernière peut vendre à d'autres organisations la propriété intellectuelle créée pour notre système. Et nous toucherons une redevance sur toutes les ventes, ce qui nous fournira une source de financement. » À ce jour, toutes les provinces du Canada s'intéressent au SIC; et aussi l'État du Maine qui en a d'ailleurs fait l'achat. Le SIC a même été présenté aussi loin qu'à Singapour.

Ce modèle audacieux vient tout simplement s'ajouter à la longue liste des innovations réalisées par la collectivité de l'IIJ au Nouveau-Brunswick — des innovations qui, selon Michael Boudreau et Robert Cyr, pourront être appliquées ailleurs.

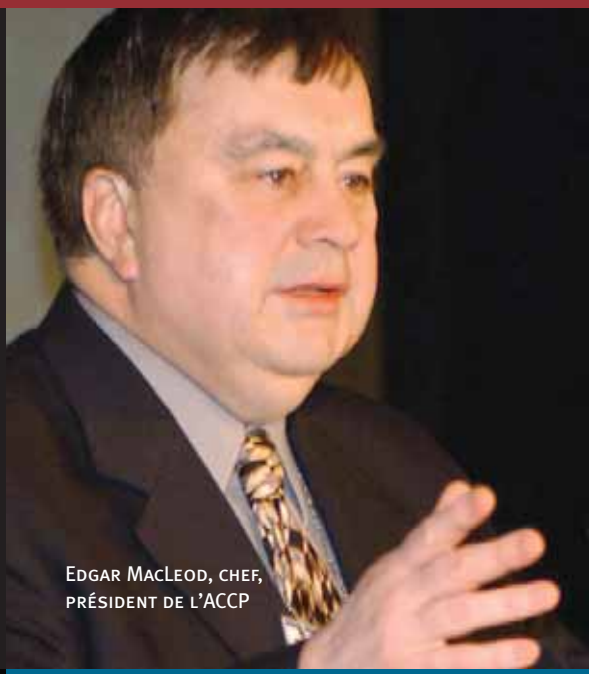
« Nous parlons du Nouveau-Brunswick comme s'il s'agissait d'un microcosme », dit M. Boudreau. « C'est un endroit formidable pour apprendre des leçons qui sont peut-être applicables à d'autres paliers. Et nous sommes tout à fait prêts et disposés à partager notre savoir. »

Rendre possible

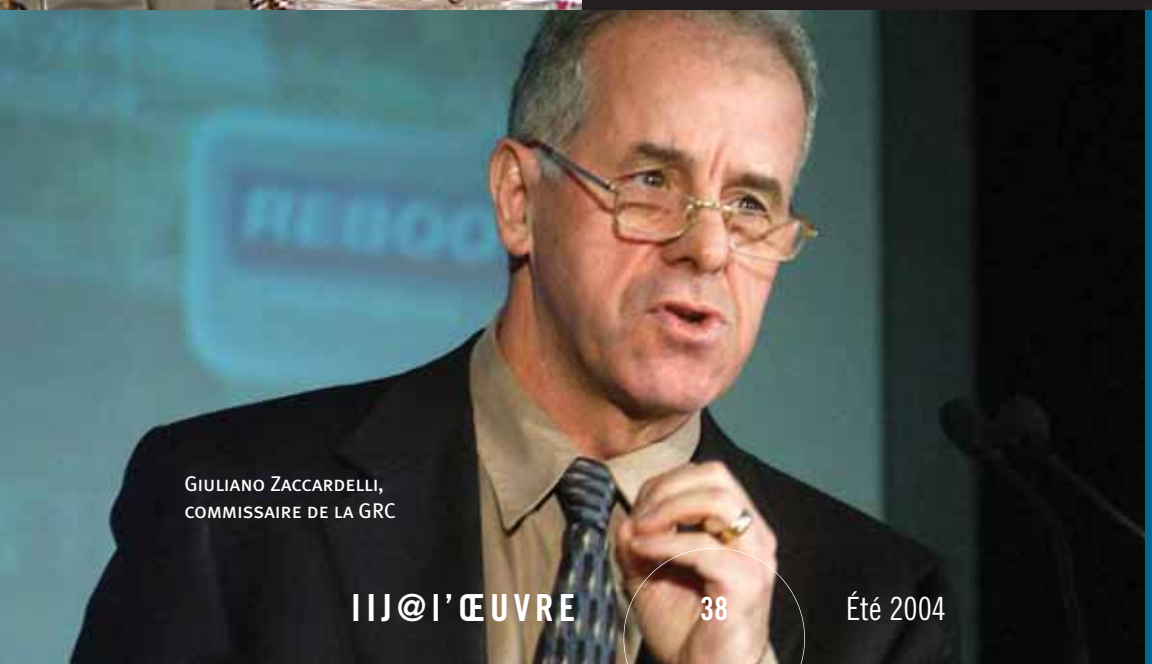
Points saillants du forum de l'ACCP sur l'échange de renseignements et l'interopérabilité



Vince Bevan, chef du Service de police d'Ottawa



Edgar MacLeod, chef, président de l'ACCP



Giuliano Zaccardelli, commissaire de la GRC

Photos reproduites avec l'aimable autorisation de l'ACCP

LA COMMUNICATION DE RENSEIGNEMENTS

« Cessez de penser que vous n'en êtes pas capables et faites-le! » Tel était l'un des principaux messages livrés lors d'une conférence nationale sur l'échange de renseignements et l'interopérabilité, organisée par l'Association canadienne des chefs de police (ACCP), qui a eu lieu du 24 au 26 novembre 2003, à Montréal, au Québec. Cette conférence d'une durée de trois jours, dont le thème était le Partenariat entre *les Services de police et les organismes d'application de la loi : Assurer le partage d'information*, devait servir de tremplin aux chefs de police et aux dirigeants des organismes d'application de la loi pour prendre des mesures immédiates afin d'améliorer les capacités d'interopérabilité et d'échange de renseignements entre les partenaires de la justice pénale au Canada.

Ce forum a attiré beaucoup de monde — dont 160 représentants de haut niveau de services de police, de gouvernements et d'organismes d'application de la loi, provenant de partout au Canada. Les participants ont eu l'occasion d'entendre un discours-programme très réfléchi prononcé par un juriste de renom, le juge Archie Campbell, lequel a présenté son point de vue sur l'échange d'information, basé sur le rapport d'enquête souvent cité sur l'affaire Paul Bernardo, dont il est l'auteur. Le juge Campbell a évoqué des affaires criminelles dans lesquelles la faible capacité d'échanger des renseignements avait nui aux efforts des policiers, et affirmé qu'un changement fondamental d'attitude s'imposait dans les services de police et les organismes d'application de la loi. « Lorsque les gens ne veulent pas échanger de renseignements, ils n'en échangent pas... C'est aussi simple que cela », a-t-il dit. Et il a ajouté que le défi des dirigeants était de trouver des moyens de motiver les membres de leur personnel à passer à l'action.

Les participants à la conférence ont également entendu toute une brochette de conférenciers invités dont le chef Edgar MacLeod (président de l'ACCP) et le ministre de la Sécurité publique du Québec, Jacques Chagnon, lesquels ont tous deux insisté sur la nécessité de surmonter les obstacles traditionnels à la mise en commun de l'information.

Dans les discussions à la table ronde et lors des séances plénières, les participants ont rappelé à maintes reprises à quel point ils estimaient important que les services de police prennent des mesures immédiates pour améliorer la communication de renseignements dans le cadre de leur travail et assurer une meilleure interopérabilité des systèmes existants.

Julian Fantino, chef du Service de police de Toronto

Photos reproduites avec l'aimable autorisation de l'ACCP

La culture policière a souvent été mentionnée comme étant un obstacle à l'atteinte de cet objectif. Les participants ont soutenu que cette culture était loin d'être une excuse pour ne pas agir, mais était plutôt appelée à jouer un rôle important dans l'avenir du système de justice pénale au Canada. Le chef de police de Toronto, Julian Fantino, a résumé la situation ainsi : « Nos actions (celles des services de police) sont examinées au microscope. On ne nous pardonnera pas d'omettre de relier les points entre eux. »

Mais reconnaître la nécessité d'améliorer l'échange de renseignements n'est qu'un aspect du défi à relever — la mise en œuvre d'une telle initiative est une tâche colossale en soi. Comme l'a fait observer Nicole Jauvin qui a déjà occupé le poste de sous-solliciteur général du Canada : « Le concept est peut-être simple, mais notre travail consiste à révolutionner la façon dont nous procédons pour retracer des individus et pour prendre les décisions quotidiennes dans l'ensemble du système de justice pénale. » Les participants à la table ronde ont évoqué à maintes reprises tout le travail qu'il restait à faire dans les domaines de la protection de la vie privée, de la technologie, des normes, de l'harmonisation des politiques et de l'élaboration de systèmes homogènes avant qu'on puisse échanger des renseignements et atteindre le niveau d'interopérabilité souhaité.

Les efforts que font actuellement les services de police de l'ensemble du Canada pour échanger des renseignements ont également été décrits dans les discussions en groupe. Ces efforts ont été mis en évidence par un groupe d'experts composé notamment du commissaire adjoint Rod Smith (GRC), de Denis Méthé (Service correctionnel du Canada), du chef Brian Collins (Service de police de London), du chef Vince Bevan (Service de police d'Ottawa), de David Douglas (Organized Crime Agency de la Colombie-Britannique) et du surintendant Dick Grattan (Équipe intégrée de la police des frontières). Chacune de ces personnes a présenté aux délégués sa propre vision des défis à relever pour mettre en œuvre, dans leurs domaines respectifs, une solution adaptée aux besoins en matière d'interopérabilité ou de communication de renseignements.

Dans les discussions à la table ronde et lors des séances plénières, les participants ont rappelé à maintes reprises à quel point ils estimaient important que les services de police prennent des mesures immédiates pour améliorer la communication de renseignements dans le cadre de leur travail et assurer une meilleure interopérabilité des systèmes existants.

Les organisateurs du forum ont également cherché à connaître directement les réactions des participants. Ils leur ont distribué un questionnaire dans lequel les répondants étaient invités à indiquer les mesures que l'ACCP devrait prendre pour assurer une meilleure communication de renseignements et une plus grande interopérabilité entre les services de police et les autres partenaires de la justice pénale au Canada. Ces questionnaires ont été remplis par les participants, puis ramassés et analysés durant la conférence de façon qu'on puisse préparer un plan d'action avant la fin du forum. Les résultats de cette enquête correspondaient aux messages qui étaient ressortis dans les discours-programmes et les discussions en groupe — la plupart des participants insistaient sur l'urgence de s'attaquer à la question de l'échange d'information.

Voici la liste des activités de suivi adoptée par les participants à la conférence :

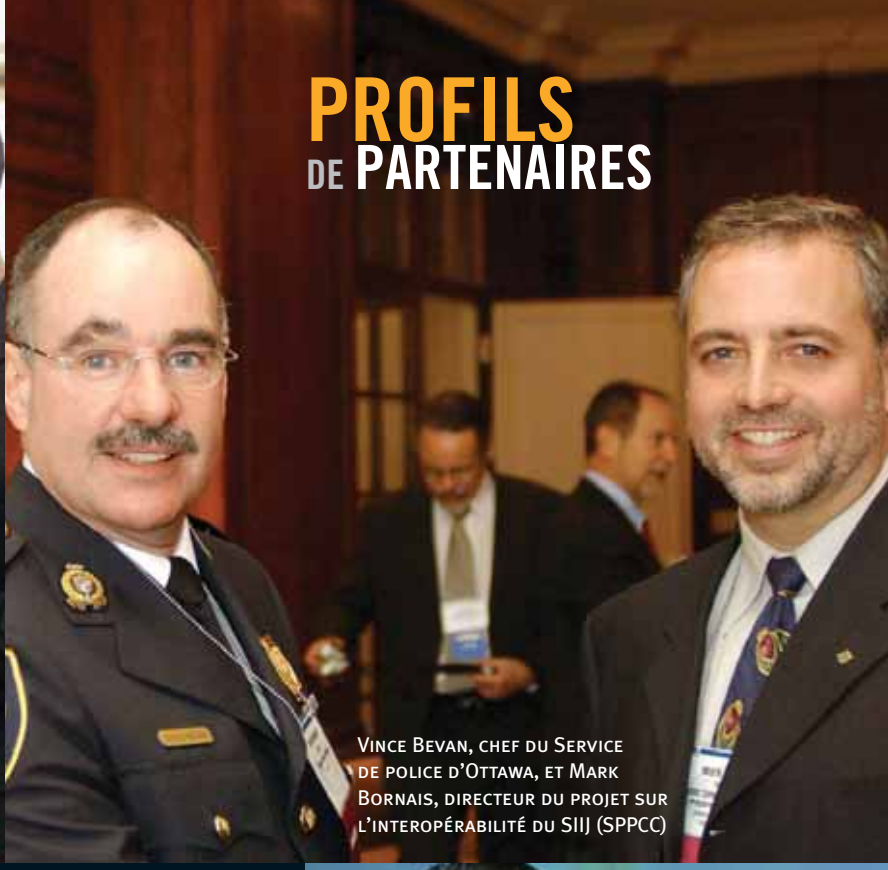
A) Pour les participants et leurs organismes respectifs :

- informer le comité exécutif des questions débattues au cours de la conférence;
- dresser un inventaire des banques d'information ainsi que des systèmes et politiques sur l'échange d'information;
- cerner les besoins opérationnels relativement aux renseignements disponibles auprès des autres organismes;
- engager des pourparlers avec d'autres organisations afin de trouver des solutions aux problèmes d'interopérabilité;
- établir un plan de migration pour la mise en application des normes de données du RCISP.

B) Pour l'ACCP :

- mener une enquête visant à déterminer où en sont les services de police et les organismes d'application de la loi dans leurs travaux de mise en application des normes de données du RCISP;
- préparer un index des installations et systèmes de connectivité existants;
- élaborer un énoncé de politique sur l'interopérabilité et l'échange d'information, et le distribuer à tous les services de police, à toutes les autorités dirigeantes et aux participants à la conférence.

Margaret Bloodworth, sous-ministre de SPPCC, et Giuliano Zaccardelli, commissaire de la GRC



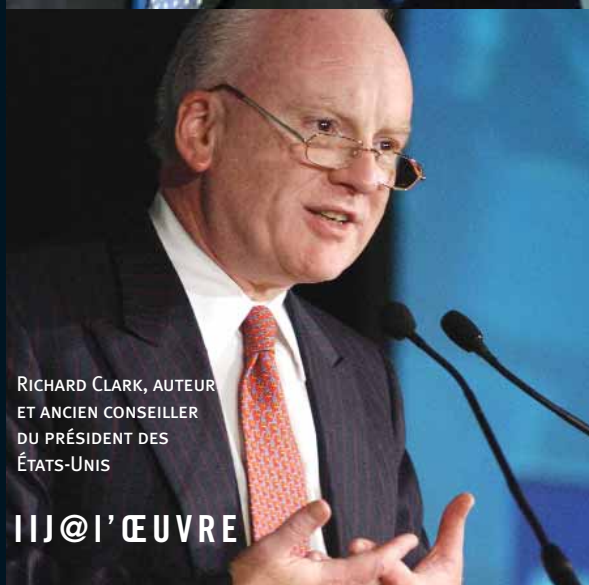
Vince Bevan, chef du Service de police d'Ottawa, et Mark Bornais, directeur du projet sur l'interopérabilité du SIIJ (SPPCC)

Photos reproduites avec l'aimable autorisation de Reboot Communications

Stratégies de transformation de la sécurité publique 2004

Points saillants de la conférence de 2004 sur les stratégies de transformation de la sécurité publique : « Technologie et lutte contre le terrorisme »

Kevin Mitnick, ex-pirate informatique, président et cofondateur de Defensive Thinking



Richard Clark, auteur et ancien conseiller du président des États-Unis

PROFILS DE PARTENAIRES

LES 26 ET 27 AVRIL 2004, DES REPRÉSENTANTS DE HAUT NIVEAU DE GOUVERNEMENTS, DE SERVICES DE POLICE, D'ORGANISMES DE SÉCURITÉ ET DU SECTEUR DE LA TECHNOLOGIE SE SONT RÉUNIS À OTTAWA AFIN D'ASSISTER À LA TROISIÈME CONFÉRENCE ANNUELLE SUR LA TECHNOLOGIE ET LA LUTTE CONTRE LE TERRORISME, INTITULÉE *STRATÉGIES DE TRANSFORMATION DE LA SÉCURITÉ PUBLIQUE 2004*, LAQUELLE ÉTAIT PRÉSENTÉE PAR LA SOCIÉTÉ REBOOT COMMUNICATIONS ET DONT LES HÔTES ÉTAIENT L'ASSOCIATION CANADIENNE DES CHEFS DE POLICE ET SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE CANADA (SPPCC); CETTE RENCONTRE DE DEUX JOURS A CONSTITUÉ, POUR DES CADRES DIRIGEANTS DU CANADA, DES ÉTATS-UNIS ET D'AUTRES PAYS, UNE OCCASION UNIQUE D'ÉTABLIR DES LIENS D'ENTRAIDE ET DE CHERCHER ENSEMBLE DES SOLUTIONS AUX PROBLÈMES DE SÉCURITÉ PUBLIQUE.

PHOTO REPRODUITE AVEC L'AIMABLE AUTORISATION DE REBOOT COMMUNICATIONS

DE GAUCHE À DROITE : JOHN PISTOLE (SOUS-DIRECTEUR ADMINISTRATIF DU FEDERAL BUREAU OF INVESTIGATION DES ÉTATS-UNIS), MARGARET BLOODWORTH (SOUS-MINISTRE DE SPPCC), GIULIANO ZACCARDELLI (COMMISSAIRE DE LA GRC), BOB MORINE (VICE-PRÉSIDENT ET DIRECTEUR GÉNÉRAL D'IBM CANADA) ET PHILLIP WEBB (PRÉSIDENT-DIRECTEUR GÉNÉRAL DE LA POLICE INFORMATION TECHNOLOGY ORGANISATION DU ROYAUME-UNI).

« Nous étions heureux que cette conférence ait lieu à Ottawa pour la première fois », a expliqué Greg Spievak, président de Reboot Communications. « L'à-propos des discussions en groupe et des discours-programmes est la marque distinctive de cette conférence annuelle sélecte, et la rencontre de cette année ne faisait pas exception à la règle. »

Les délégués ont assisté à plus de 30 présentations faites par des experts internationaux de renom. Les conférenciers représentant le gouvernement du Canada comprenaient entre autres Margareth Bloodworth, sous-ministre de SPPCC, laquelle a donné un aperçu des activités de son ministère et des priorités à court terme de celui-ci en matière de sécurité publique, ce qui englobe l'interopérabilité, la politique nationale de sécurité, l'accès légal ainsi que les mesures visant à améliorer l'infrastructure de base et à assurer la sécurité informatique. Des renseignements supplémentaires plus détaillés concernant le projet sur l'interopérabilité, lancé récemment, ont été présentés séparément par le directeur de ce projet, Mark Bornais (Secrétariat de l'intégration de l'information de la justice, SPPCC).

L'importance primordiale de favoriser une meilleure interopérabilité a été soulignée à maintes reprises durant les discours-programmes et les discussions en groupe. Les conférenciers ont fait observer que les gouvernements du Canada, des États-Unis et d'autres pays devaient relever le défi d'amener différents organismes à s'échanger des renseignements sans mettre en péril la protection de la vie privée ou la sécurité de leurs propres systèmes. À cet égard, diverses solutions ont été proposées dans les présentations ainsi que par les nombreux fournisseurs présents dans la salle d'exposition attenante aux salles où se réunissaient les participants à la conférence; les solutions proposées comprenaient entre autres des systèmes d'authentification de l'utilisateur, le cryptage des données et la connectivité sans fil.

Les dirigeants des services de police et des organismes de sécurité nationale du Canada et de toutes les parties du monde étaient également bien représentés dans les discussions en groupe; mentionnons notamment la participation à ces discussions du commissaire de la GRC, Giuliano Zaccardelli, du chef Edgar MacLeod (président de l'ACCP), du chef Vince Bevan (Service de police d'Ottawa), de John Pistole (sous-directeur administratif du Federal Bureau of Investigation des États-Unis) et de Phillip Webb (président-directeur général de la Police Information Technology Organization du Royaume-Uni). Les présentations de ces dirigeants ont permis aux délégués d'entrevoir et de comprendre comment les Services de police pouvaient améliorer la communication de renseignements à l'échelle nationale et internationale. Des méthodes précises pour surmonter les obstacles à l'échange de renseignements ont également été discutées lors des échanges en groupe.

Étant donné que cette conférence annuelle était d'envergure internationale, les délégués ont eu droit à deux discours-programmes spéciaux. Le premier a été prononcé par Richard Clarke, l'auteur du livre *Against All Enemies: Inside America's War on Terror*, et ancien conseiller du président américain sur la lutte contre le terrorisme. Dans son allocution, M. Clarke a insisté tout particulièrement sur le fait que la technologie actuelle donne aux gouvernements des capacités et un accès potentiel à l'information sans pareil, et soutenu que cette question devrait être approfondie en élargissant le dialogue avec la société civile.

Le deuxième discours-programme spécial a été prononcé par Kevin Mitnick, un ex-pirate informatique de renommée internationale, qui a déjà été considéré comme l'escroc informatique le plus recherché dans l'histoire des États-Unis. Les différentes études de cas présentées par M. Mitnick montraient fort bien pourquoi les organismes doivent doubler leurs mesures de protection des renseignements personnels afin de mettre ceux-ci à l'abri des pirates informatiques et autres intrus qui cherchent à utiliser cette information à leur avantage.

Au dire de tous, la conférence *Stratégies de transformation de la sécurité publique 2004* a été un grand succès. Compte tenu de la réussite de cette rencontre et des rencontres antérieures (qui ont eu lieu à Whistler, en Colombie-Britannique, en 2002, et à Bal Harbour, en Floride, en 2003), la quatrième conférence annuelle, celle de 2005, aura lieu à San Francisco, en Californie.

Des renseignements détaillés sur la conférence de 2005 seront bientôt disponibles sur le site Web de la société Reboot Communications : **www.rebootcanada.com**.

UNE VOLONTÉ COMMUNE DE SE BRANCHER

Le point sur les partenariats et les efforts concertés du Canada et des États-Unis en matière de sécurité publique

En travaillant ensemble, à titre de partenaires, les ministères fédéraux, provinciaux et territoriaux ainsi que les organismes responsables de la justice pénale et de la sécurité publique au Canada témoignent, en fait, d'une *volonté commune* de se brancher et d'échanger des renseignements de manière efficace, sûre et fiable.

Du Justice Enterprise Information Network (JEIN) de la Nouvelle-Écosse à l'Équipe d'intégration des systèmes de la justice du Manitoba, et du Justice Information System (JUSTIN) de la Colombie-Britannique au projet québécois de système intégré d'information de justice — pour ne nommer que quelques initiatives — la volonté d'atteindre les objectifs d'intégration de l'information de la justice et d'interopérabilité des systèmes d'information est manifeste partout au pays. Les différentes réalisations des partenaires de tous les paliers de gouvernement témoignent des progrès importants faits dans l'intérêt de la sécurité publique au Canada.

Grâce aux efforts déployés à ce jour en matière d'intégration de l'information de la justice, les partenaires du RCISP, y compris Sécurité publique et Protection civile Canada (SPPCC), ont appris énormément les uns des autres.

Pour assurer la viabilité de ce formidable lieu d'apprentissage, le dialogue demeure un élément clé.

Afin d'appuyer et de favoriser les partenariats entre les organismes membres du RCISP, la Division des partenariats du Secrétariat de l'intégration de l'information de la justice entend saisir les nombreuses occasions de poursuivre ce dialogue en 2004 :

- réunions (spéciales et annuelles) du Réseau du leadership fédéral, provincial et territorial (FPT) pour l'intégration de l'information de la justice, qui ont lieu depuis 2001 et qui comprennent des échanges en personne et dans le cadre de téléconférences, afin de faire le point sur l'interopérabilité et la communication de renseignements. La prochaine rencontre annuelle de ce groupe doit avoir lieu à Ottawa, en juin 2004;
- élaboration d'une *approche nationale de l'échange d'information* — en partenariat avec des représentants fédéraux, provinciaux et territoriaux (FPT) — visant à convaincre les ministres FPT de la Justice de signer officiellement une déclaration commune en vue de conclure un accord national sur l'échange d'information;
- consultations avec des partenaires provinciaux de la Saskatchewan et de la Nouvelle-Écosse afin de recueillir leurs points de vue et leurs suggestions concernant un document de politique ministérielle intitulé *Cadre de gestion de l'information*;
- prise de dispositions en vue de la participation de Margaret Bloodworth, sous-ministre de SPPCC, au forum d'avril 2004 sur la sécurité publique et la lutte contre le terrorisme dont le thème était *Stratégies de transformation de la sécurité publique — Terrorisme et technologie : Prévention, protection et poursuites* (et dont l'hôte était l'Association canadienne des chefs de police).

La collaboration avec les États-Unis est tout aussi importante — comme en témoignent la Déclaration sur la frontière intelligente Canada-États-Unis et le Forum sur la criminalité transfrontalière Canada–États-Unis, un événement annuel. Les deux pays sont très désireux d'étudier les questions touchant l'interopérabilité entre les services d'application de la loi le long de la frontière commune. L'utilisation de normes de données communes est perçue comme un élément clé de l'amélioration de l'interopérabilité.

L'adoption de telles normes permet non seulement d'accroître l'efficacité du système de sécurité déjà bien géré en place à la frontière du Canada et des États-Unis, mais aussi de corriger les lacunes de ce système. En voici des exemples :

- le Programme NEXUS, de l'Agence des services frontaliers du Canada, lequel simplifie le passage à la frontière des voyageurs approuvés au préalable, est maintenant opérationnel dans dix postes frontaliers et sera étendu sous peu à trois autres postes;
- le Programme d'expéditions rapides et sécuritaires (le Programme EXPRESS), de l'Agence des services frontaliers du Canada, est maintenant opérationnel dans 12 postes frontaliers dans lesquels le volume d'activités commerciales est très élevé, représentant 80 % du trafic commercial entre le Canada et les États-Unis;
- Sécurité publique et Protection civile Canada continuera d'examiner des façons de tirer profit des succès obtenus à ce jour, en collaborant étroitement avec les États-Unis, d'une façon compatible avec les préoccupations relatives à la protection de la vie privée, avec les droits de la personne et avec le droit canadien.

SUITE DE LA PAGE 21

Mais M. Francœur affirme que les différences sont tellement minimes que le système peut établir avec une précision raisonnable qu'il s'agit bel et bien de la même personne.

« Durant notre étude, nous avons relevé les effets d'une vingtaine de caractéristiques des photos sur la précision de la reconnaissance faciale », explique-t-il, « tous les aspects, allant de la luminosité au vieillissement et aux poils faciaux. Je me suis même porté volontaire pour que l'on prenne une photo de moi rasé de près et une autre avec une longue barbe. Mais la configuration du système peut être ajustée pour traiter ces variantes de manière intelligente ».

Fait important, M. Francœur souligne qu'aucun système de reconnaissance faciale ne pourrait prendre de décisions strictement automatisées. Lorsque qu'une photo semble concorder avec celle d'une personne dont le nom figure sur une liste de surveillance dans une banque de données, un agent de sûreté est averti et invité à pousser l'examen un peu plus loin.

« Pour nous, cela constitue un avantage par rapport à la dactyloscopie », dit M. Francœur. « Lorsque vous utilisez les empreintes digitales comme identificateur, vous devez être extrêmement compétent pour effectuer les vérifications nécessaires lorsque vous croyez être en présence d'un faux positif ou confirmer une authentique concordance positive. Il est beaucoup plus facile de former les gens à comparer et évaluer des photos. »

À QUOI RESSEMBLE L'AVENIR?

Durant son étude, le Bureau des passeports a confirmé que la technologie de la reconnaissance faciale était suffisamment au point, efficace et perfectionnée pour que son déploiement soit envisagé. M. Francœur et son équipe ont présenté un rapport d'analyse de rentabilisation favorable au Commissariat à la protection de la vie privée afin qu'il en fasse l'examen.

« J'ai très hâte de voir comment le rapport d'analyse de rentabilisation sera accueilli », dit M. Francœur. « Nous sommes convaincus que la technologie de la reconnaissance faciale répondra à nos besoins et nous aidera à contrer les menaces réelles qui pèsent sur la sécurité canadienne. Et c'est l'assurance que souhaitent obtenir toutes les personnes qui demandent un passeport canadien : être en possession d'un document sécurisé, accepté à l'échelle internationale. »