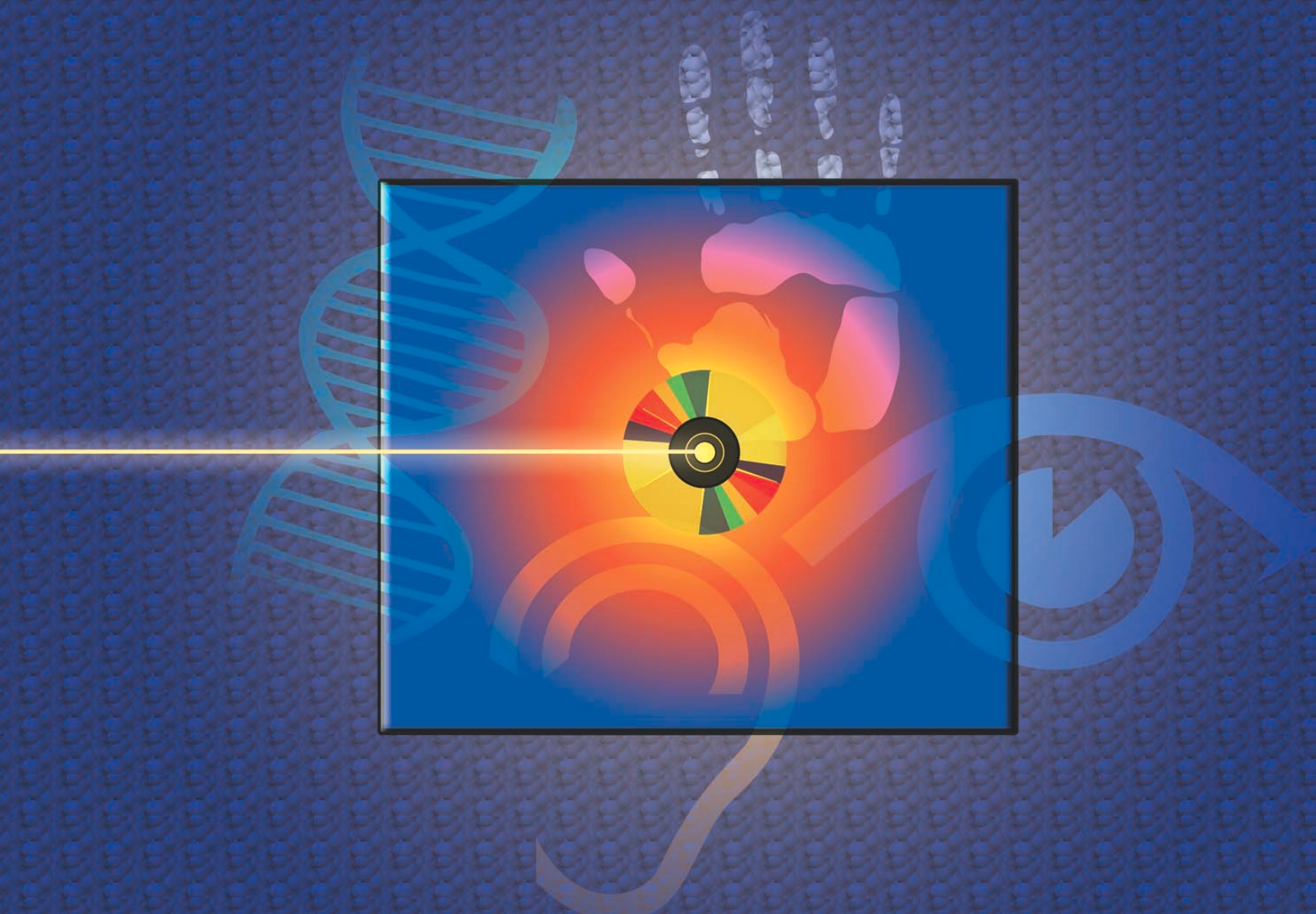
COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

DOCUMENT DE **CONSULTATION**

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques



Québec

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

Document de consultation

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques

Commission de l'éthique de la science et de la technologie
1200, route de l'Église
3e étage, bureau 3.45
Sainte-Foy (Québec)
G1V 4Z2

Réalisation

Diane Duquet, coordonnatrice de la CEST

Mise en pages

Lauraine Bérard

Conception graphique de la couverture

Créativité Sylvain Vallières Inc.

Dépôt légal : 2e trimestre 2005
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada

ISBN 2-550-44626-7

Pour faciliter la lecture du texte, le genre masculin est utilisé sans aucune intention discriminatoire.

LES MEMBRES DE LA COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

PRÉSIDENTE

M^e Édith Deleury
Professeure – Faculté de droit
Université Laval

MEMBRES

Patrick Beaudin
Directeur général
Société pour la promotion de
la science et de la technologie

Louise Bernier
Doctorante en droit (bioéthique, génétique et droit)
Université McGill

Sabin Boily
Consultant en nanotechnologies

D^r Pierre Deshaies
Médecin spécialiste en santé communautaire
Chef du département clinique de santé publique
Hôtel-Dieu de Lévis

Benoît Gagnon
Chercheur
Chaire Raoul-Dandurand en études stratégiques et diplomatiques
Université du Québec à Montréal

Jacques T. Godbout
Sociologue
Institut national de la recherche scientifique – Urbanisation, Culture et Société

Michèle S. Jean
Faculté des études supérieures
Université de Montréal
Présidente du Comité international de bioéthique – UNESCO

Johane Patenaude
Professeure (éthique) – Faculté de médecine
Université de Sherbrooke

François Pothier
Professeur – Faculté des sciences de l'agriculture et de l'alimentation
Université Laval

Louise Rozon
Directrice
Option Consommateurs

D^r Stanley Vollant
Médecin
Complexe hospitalier de la Sagamie
Saguenay

MEMBRES INVITÉS

Geneviève Bouchard
Sous-ministre adjointe et directrice générale
Direction générale des politiques
Ministère de l'Emploi, de la Solidarité sociale et de la Famille
Gouvernement du Québec

Danielle Parent
Secrétaire adjointe à la législation et conseillère juridique
Commission d'accès à l'information du Québec

COORDONNATRICE

Diane Duquet

TABLE DES MATIÈRES

INTRODUCTION

À n'en pas douter, les événements du 11 septembre 2001 ont changé la donne en matière de sécurité, que ce soit à l'échelle nationale ou internationale. Parce qu'ils estiment essentiels de le faire ou sous la pression des États-Unis – notamment dans le contrôle des voyageurs – les gouvernements nationaux sont appelés à revoir comment s'exerce la sécurité sur leur territoire et quelles sont les mesures mises en place (ou à mettre en place) pour contrer le terrorisme.

Outre le terrorisme, cependant, les États doivent également contrer la criminalité sur leur territoire, notamment en ce qui a trait au vol d'identité à des fins de consommation et à l'usurpation d'identité dans l'obtention de services gouvernementaux offerts aux citoyens résidents. Comme d'autres gouvernements à travers le monde, le Canada est amené à considérer l'utilisation de données biométriques pour le contrôle de ses frontières. Mais il s'y intéresse aussi dans le cadre de la mise en place d'une politique nationale en matière d'identité souhaitant faire de la biométrie une partie intégrante des pièces d'identité délivrées par le gouvernement canadien.

L'application de technologies nouvelles dans l'implantation de moyens de surveillance des personnes et de contrôle de l'identité constitue donc l'essence des nouvelles approches gouvernementales, mais également organisationnelles en matière de sécurité – certaines entreprises y ayant recours dans le contrôle des accès à des sites matériels ou électroniques. Et ces technologies nouvelles, souvent intrusives – sur le plan du consentement, de la vie privée et de l'intégrité corporelle – reposent majoritairement sur la collecte et le stockage d'informations personnelles et l'utilisation de données biométriques.

C'est ce contexte d'une intensification des mesures de contrôle et de la disponibilité croissante de système biométriques de toutes sortes pour établir ou valider l'identité d'une personne qui amène la Commission de l'éthique de la science et de la technologie à s'interroger sur les enjeux éthiques associés à une telle situation. Et à poser la question suivante, fondamentale sur le plan de l'éthique: y a-t-il corrélation entre les moyens de contrôle et de surveillance mis en place ou envisagés grâce à la technologie biométrique et la finalité recherchée?

Le présent résumé rappelle brièvement les points saillants du *Document de réflexion*[1] préparé par la CEST sur le sujet et présente les grandes lignes du questionnement éthique qu'elle soumet pour consultation. Dans une étape ultérieure et en s'inspirant des commentaires recueillis lors de sa consultation, la Commission remettra au gouvernement et rendra public un avis sur les enjeux éthiques associés à l'utilisation des données biométriques à des fins de sécurité, accompagné de recommandations à l'intention des divers acteurs concernés.

1. LA NOTION DE « SÉCURITÉ »

Assurer la sécurité d'un territoire, d'un pays, d'une ville, d'une habitation est un défi constant car il faut d'une part déterminer correctement les menaces et d'autre part mettre en place un système efficace de protection. À l'heure actuelle, surtout depuis l'attentat de 2001, les paramètres du danger et de la sécurité semblent entièrement nouveaux et paraissent exiger la mise en place de mesures également nouvelles tant sur le plan technique que politique.

Quatre questions clefs jalonnent le débat sur la notion de sécurité : « Quelle est la nature de l'insécurité? »; « À quel objet la sécurité fait-elle référence? »; « Qui en assume la responsabilité? »; « Quels sont les moyens d'assurer la sécurité? »[2]. Traditionnellement, la sécurité sociétale faisait référence au concept de sécurité nationale. La sécurité était définie par la stratégie, qui servait essentiellement à préserver la souveraineté nationale et à préserver ou à

[1] Disponible en fichier pdf sur le site de la Commission : http://ethique.gouv.qc.ca.
[2] Isabelle MASSON, « Sécurité », in Alex MACLEOD, Evelyne DUFAULT et F. Guillaume DUFOUR (dir.), *Relations internationales : théories et concepts* , Montréal, Athéna éditions, 2004, p.216.

augmenter la puissance étatique par les moyens militaires, politiques et économiques. Dorénavant, la sécurité transcende divers domaines et a des objectifs multiples. Ainsi, la sécurité apparaît à la fois comme un bien à atteindre, un bien indispensable à la vie, mais aussi comme une stratégie mise en œuvre pour que la sûreté soit acquise. En prétendant protéger, l'État en vient aussi à contrôler même au-delà du nécessaire. D'où un conflit permanent entre la requête de sécurité de l'individu et la requête de liberté suivant laquelle chaque personne peut disposer librement d'elle-même en toute circonstance: un défi technique s'il en est, mais aussi une question à caractère politique et éthique.

2. LA TECHNOLOGIE BIOMÉTRIQUE

Mises à part l'utilisation des empreintes digitales dans le système judiciaire pour déterminer ou confirmer l'identité d'une personne et, plus récemment, celle de lecteurs de la main comme moyens de contrôle de l'accès à ou dans certains édifices, les technologies biométriques sont généralement peu connues de la population.

Dans le domaine de la sécurité, **la biométrie** désigne l'ensemble des moyens techniques qui permettent de reconnaître une personne à partir de certaines de ses caractéristiques biologiques ou comportementales. Grâce aux technologies de l'information, ces données biométriques mesurables peuvent être conservées sur un support électronique autonome (une puce électronique, par exemple ou un disque dur) ou dans une banque de données privée ou en réseau.

La biométrie peut servir, entre autres, à des fins d'**identification** (qui est la personne qui possède telle caractéristique biométrique?) ou d'**authentification** d'une personne (une personne est-elle bien celle qu'elle prétend être? ses caractéristiques biométriques confirment-elles son identité?)

La distinction entre ces deux finalités est importante car, selon la caractéristique biométrique retenue et son mode de stockage (information centralisée dans une banque de données ou inscrite sur un support informatique ou non), mais aussi selon les objectifs poursuivis, le risque pour la protection de la vie privée et des renseignements personnels pourra différer.
Les systèmes biométriques sont généralement classés en fonction de trois catégories de données particulières à une personne:

- ***des données morphologiques ou physiologiques***, comme la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la voix, de la rétine (dessin du réseau veineux de l'œil), de l'iris de l'œil et la thermographie.
- ***les données comportementales***, comme la dynamique de la signature, de la frappe au clavier d'ordinateur, la façon de marcher, etc.
- ***des données biologiques***, comme l'empreinte génétique (ADN), l'odeur, la salive, l'urine, etc.

Le tableau ci-dessous résume les caractéristiques des principales données biométriques pouvant être utilisées à des fins d'identification et d'authentification[3].

[3] Information tirée de Bernard DIONNE et ÈVELYNE RACETTE, « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », Ministère des Relations avec les citoyens et de l'Immigration, Québec, mars 2004 – document d'information, p. 21-37.

Donnée biométrique	Avantages	Inconvénients	Applications
Empreintes digitales	▪ technologie la plus éprouvée techniquement et la plus connue du grand public ▪ petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones cellulaires, PC) ▪ faible coût des lecteurs ▪ traitement rapide ▪ bon compromis entre les faux rejets et les fausses acceptations.	▪ image « policière » ▪ difficulté de lecture avec des doigts sales ou abîmés ▪ besoin de la coopération de la personne concernée (pose correcte du doigt sur le lecteur) ▪ certains systèmes peuvent être trompés par un moulage de doigt ▪ environ 2 % de la population mondiale ont des empreintes difficilement exploitables	▪ en théorie, toutes les applications possibles, mais le capteur est exposé à une éventuelle dégradation dans les applications grand public (distributeur de billets, accès extérieur à des locaux, …) ▪ contrôle d'accès physique (locaux, machines, équipements spécifiques, contrôle d'accès logique – système d'information) ▪ identification judiciaire gestion des titres délivrés (permis de conduire, passeport, carte d'identité nationale)
Reconnaissance faciale	▪ seule une opération chirurgicale intervenant sur le cartilage est en mesure de la tromper ▪ n'est pas intrusive et n'exige aucun contact physique avec le capteur	▪ sensible à la variation de l'éclairage et au changement de la position du visage lors de l'acquisition de l'image ▪ taux élevés de fausses acceptations ou faux refus ▪ se fait souvent à l'insu de la personne	▪ contrôle d'accès physique (locaux, machines, équipements spécifiques, contrôle d'accès logique – système d'information) ▪ identification judiciaire (aéroports, casinos, centres commerciaux, stades, etc.) gestion des titres délivrés (gestion des permis de conduire aux États-Unis)
Géométrie de la main	▪ très simple à utiliser ▪ technique moins capricieuse que la reconnaissance d'empreintes digitales : le taux d'humidité, la saleté et les petites coupures n'empêcheront pas le système de fonctionner ▪ pas de traces de la géométrie de la main laissées partout ▪ niveaux très raisonnables d'exactitude	▪ trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone ▪ sujet aux modifications de la forme de la main liées au vieillissement ▪ taux de fausses acceptations élevé pour des jumeaux ou d'autres membres de la même famille	▪ contrôle d'accès à des locaux ou à des sites (Disney World, J.O. d'Atlanta, Aéroports de San-Francisco et de Tel Aviv, Université de Georgia, etc.) ▪ Horodateur
Reconnaissance de l'iris	▪ très grande fiabilité ▪ grande quantité d'informations contenue dans l'iris ▪ vrais jumeaux non confondus ▪ caméra moins exposée qu'un capteur avec contact (empreintes) mais davantage qu'un micro (voix) ▪ faible taux d'erreur pour les produits haut de gamme (méthode très fiable) ▪ le fleuron de la biométrie	▪ aspect psychologiquement invasif de la méthode ▪ les contraintes sur l'éclairage demandent souvent que le capteur soit proche de l'œil. Les variations de l'éclairage ambiant et les reflets perturbent fortement la mesure ▪ les systèmes bas de gamme peuvent être trompés à partir d'une photo ou d'une lentille de contact ▪ la technologie n'est pas encore suffisamment simple d'utilisation pour permettre le contrôle d'accès sur les postes clients	▪ distributeurs de billets de banques ▪ contrôle d'accès physique (locaux, machines, équipement spécifiques, contrôle d'accès logique – systèmes d'information critiques)

Donnée biométrique	Avantages	Inconvénients	Applications
Reconnaissance de la rétine	▪ réputé comme étant le plus fiable des moyens biométriques ▪ carte vasculaire, propre à chaque individu (diffère entre deux jumeaux) et évolue peu avec l'âge ▪ l'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure) ▪ faibles taux de faux rejets et de fausses acceptations ▪ résistant à la fraude ▪ faible taille du fichier signature : 96 octects (512 pour l'iris)	▪ mauvaise acceptation du public (l'œil est un organe sensible). Réticence psychologique de l'usager. On accepte difficilement l'idée d'un rayon lumineux, même inoffensif, dans l'œil ▪ nécessité de placer ses yeux à proximité d'une tête de lecture (à moins de 4 cm.) ▪ méthode qui requiert des sujets coopératifs et entraînés ▪ technologie pas encore suffisamment simple d'utilisation pour permettre le contrôle d'accès sur les poste clients ▪ coûteux	▪ contrôle d'accès à des locaux vulnérables ▪ distributeurs automatiques de billets ▪ identification judiciaire
Reconnaissance de la voix	▪ plus facile de protéger le capteur que dans les autres technologies ▪ technologie non intrusive qui n'exige aucun contact physique avec le capteur ▪ permet l'identification à distance au moyen d'une liaison téléphonique	▪ sensible à l'état physique de la personne. La fatigue, le stress ou un rhume peuvent provoquer des variations de la voix ▪ dégradation croissante des performances au fur et à mesure que le temps augmente entre la session d'enregistrement et la session de contrôle ▪ le comportement des locuteurs se modifie lorsque ceux-ci s'habituent au système ▪ fraude possible par enregistrement ▪ sensible aux bruits ambiants; nécessite une excellente qualité audio ▪ taux élevé de faux rejets et de fausses acceptations	▪ « sur site » : serrures vocales pour contrôle d'accès, cabines bancaires en libre service ▪ liées aux télécommunications : identification du locuteur à travers le réseau téléphonique pour accéder à un service ▪ judiciaires : pour la recherche de suspects, orientation d'enquêtes, preuves lors d'un procès.
Reconnaissance de la signature	▪ culturellement ergonomique car la signature est un geste commun de la vie courante ▪ produit une représentation visuelle de la signature ▪ apporte une certaine sécurité sans nécessairement imposer la vérification systématique de la signature ▪ actuellement la seule technologie classée comme comportementale qui a véritablement abouti	▪ signature instable (certaines personnes ont une signature très erratique) ▪ la signature peut aussi changer sensiblement dans le temps (au bout de quelques années) ▪ sensible à l'état physique de la personne: la fatigue et le stress peuvent provoquer des variations dans la signature ▪ peut être imitée avec de l'entraînement ▪ mesure d'identification très restrictive	▪ contrôle d'accès logique

Donnée biométrique	Avantages	Inconvénients	Applications
Dynamique de la frappe au clavier	▪ très convivial	▪ vitesse de frappe instable (peut être très erratique chez certaines personnes) ▪ sensible à l'état physique de la personne: la fatigue et le stress peuvent provoquer des variations dans la vitesse ▪ mesure d'identification très restrictive	▪ contrôle d'accès logique ▪ commerce électronique
Le profil génétique (ADN)	▪ technologie très fiable	▪ les techniques d'analyse sont chimiques pour le moment ▪ tests actuels très intrusifs	▪ identification judiciaire
Thermographie	▪ pas intrusive	▪ très coûteuse	▪ expérimental

Le marché de la biométrie est en pleine expansion et peut exercer une pression sur la prise de décision relative à l'utilisation des données biométriques à des fins de sécurité. À l'heure actuelle, le secteur est largement dominé par les sociétés américaines et la technologie relative aux empreintes digitales.

De façon générale, la population canadienne serait favorable aux identificateurs biométriques (sondage pancanadien de novembre 2002); certains croient cependant que l'utilisation de cette technologie irait à l'encontre des valeurs de liberté et d'équité (36 %) et nuirait à la protection des renseignements personnels (53 %). La création d'une « infrastructure de surveillance » fait également partie des préoccupations mentionnées lors d'un Forum tenu par Citoyenneté et Immigration Canada en novembre 2003, et toute intrusion de l'État est perçue « comme une action répréhensible, une invasion de l'espace privé, et l'antithèse des principes d'une société libre et ouverte où les valeurs sont tout aussi importantes que l'avancement des technologies. »

Outre la nature technique, politique et juridique du débat, la Commission considère qu'il est aussi en grande partie de nature éthique. Est-il acceptable qu'au nom de la sécurité des biens et des personnes les gouvernements puissent accéder aux données biométriques à caractère personnel des citoyens et qu'ils puissent le faire à d'autres fins que celles pour lesquelles elles ont été initialement fournies? Est-il acceptable de passer d'un mode sécuritaire « réactif » (fondé sur le consentement) à un mode « proactif » qui favorise l'utilisation de systèmes d'information en facilitant la collecte de renseignements personnels ? De telles mesures de contrôle sont-elles proportionnelles aux finalités recherchées : contrer le terrorisme international, la criminalité et l'usurpation d'identité à l'intérieur du pays?

3. LE CONTEXTE DES APPLICATIONS BIOMÉTRIQUES : LA MISE EN PLACE DE MESURES DE SÉCURITÉ

La revue de littérature qu'a réalisée la Commission démontre que le sujet de l'utilisation des données biométriques à des fins de sécurité nationale et internationale est d'actualité et que plusieurs gouvernements dans le monde se penchent sur la question. De l'avis général, les consensus en la matière sont difficiles à réaliser et les décisions auront, dans certains cas, une portée internationale (c'est déjà le cas avec les exigences américaines en matière de passeport).

3.1 La sécurité internationale : combattre le terrorisme

Depuis le 11 septembre, un grand nombre de pays se posent la même question : comment échapper aux attentats terroristes et contrer le terrorisme international? Le terrorisme et ses

menaces obligent les gouvernements à recourir à des mesures qui englobent la masse des citoyens honnêtes et respectueux de l'État de droit, sans pour autant offrir de garanties de succès et avec des conséquences sociales et éthiques lourdes pour le pluralisme des sociétés modernes et le respect de la démocratie.

Au nombre des éléments qui ressortent de son tour d'horizon sur le terrorisme international et sur les mesures mises en place pour tenter de le contrer, la Commission retient les points suivants :

- le caractère insaisissable de l'attaquant;
- la diversité, la perversité et l'ampleur des attentats qui peuvent être perpétrés;
- l'existence d'une cause, d'une idéologie qui sous-tend les attaques;
- l'incapacité à prévoir où, quand, comment se fera le prochain attentat;
- les gains réalisés au détriment de la démocratie;
- le nombre et la diversité des mesures mises en place pour combattre le terrorisme;
- la discrimination latente ou affichée à l'égard de certains groupes qui en résulte.

Ce sont des éléments qu'il importe de garder à l'esprit au regard de la technologie biométrique et de son utilisation pour contrer le terrorisme international et pour répondre aux questions suivantes: y a-t-il corrélation entre les moyens utilisés ou envisagés et la finalité recherchée – en d'autres mots, la biométrie représente-t-elle un instrument adéquat pour contrer le terrorisme à l'échelle internationale ou nationale? les mesures mises en place qui n'ont pas recours à cette technologie pourraient-elles être suffisantes?

3.2 La sécurité intérieure : garantir l'identité des personnes

Selon le Solliciteur général du Canada, « le vol d'identité est devenu l'une des formes de crime qui connaît la croissance la plus rapide au Canada et aux États-Unis. » Ce type de criminalité peut constituer un problème individuel (un citoyen victime d'une usurpation d'identité) mais aussi, à plus large échelle, un problème collectif d'usage abusif des services gouvernementaux offerts à la population grâce aux contributions des citoyens.

Il existe deux grandes catégories de documents utilisés pour confirmer l'identité ou le statut d'une personne au Canada : les documents primaires (certificats de naissance et de décès, documents d'immigration et de citoyenneté) et les documents d'admissibilité (passeports, cartes d'assurance sociale, cartes d'assurance maladie), qui donnent lieu à un partage des responsabilités entre le gouvernement fédéral et les gouvernements provinciaux. Dans son document d'information préparé pour les fins du forum d'octobre 2003, Citoyenneté et Immigration Canada mentionnait que le recours à la biométrie était considéré pour rehausser l'intégrité des pièces d'identité délivrées sous sa responsabilité.

À quel point le recours aux données biométriques permettra-t-il de contrer le problème du terrorisme et d'arrêter aux frontières un éventuel terroriste? De plus en plus, semble-t-il, le recrutement de terroristes se fait auprès des citoyens de pays visés par une attaque possible, nouvellement convertis à des mouvements extrémistes de type religieux ou partageant l'idéologie terroriste. Qu'y changera la biométrie?

D'ici 2015, plus d'un milliard de personnes pourraient faire partie d'une immense base de données mise en place à la demande de l'OACI à des fins de reconnaissance faciale des voyageurs. Au Canada, la Commissaire à la protection de la vie privée constate que « la fréquence croissante avec laquelle les renseignements personnels circulent par-delà les frontières, dans des économies interdépendantes de plus en plus mondialisées, a d'importantes répercussions sur la protection de la vie privée des Canadiens et des Canadiennes. Nous avons le devoir de protéger les renseignements personnels des Canadiens et des Canadiennes. Il nous faut une stratégie équilibrée et sensée de protection des renseignements personnels. »

3.3 La sécurité matérielle ou virtuelle : contrôler l'accès aux sites

L'accès à des sites comporte deux segments d'intérêt : l'accès physique et l'accès informatique. L'accès physique concerne le contrôle de l'accès à une entité matérielle (grandes infrastructures, immeubles, bureaux, gymnases, bibliothèques ou tout autre lieu). L'accès informatique concerne le contrôle de l'accès à un ordinateur, à un serveur, à un logiciel ou à un service informatique.

L'utilisation de plus en plus répandue de données biométriques pour contrôler l'accès à des sites physiques ou informatiques est-elle toujours justifiée, ne risque-t-elle pas de mener à une banalisation des caractéristiques biométriques de chaque citoyen?

3.4 La sécurité : une justification à la surveillance tous azimuts?

La Commission estime qu'elle ne peut passer sous silence d'autres moyens de contrôle et de surveillance qui, strictement parlant, ne reposent pas sur une utilisation de données biométriques, mais soulèvent néanmoins la question d'une intrusion possible de l'État et des organisations dans la vie privée des citoyens et des travailleurs, notamment la vidéosurveillance et la cybersurveillance. Au même titre que le recours aux données biométrique, la mise au point de ces divers dispositifs soulève aussi la question de la proportionnalité des moyens par rapport à la finalité et le respect de la vie privée de chacun.

Plusieurs craignent aujourd'hui l'avènement d'une société sous surveillance et l'omniprésence de « Big Brother ». Les mesures mises en place ou envisagées pour assurer la sécurité du territoire, celle des citoyens et celle des entreprises, portent à croire que le scénario n'est pas surréaliste. Au nom de la sécurité, il apparaît aujourd'hui possible d'avoir des exigences moindres à l'égard de la protection des renseignements personnels et de leur confidentialité, du droit à la vie privée et des libertés civiles. Faut-il que ce soit le cas? Peut-il exister un équilibre entre la sécurité et les libertés individuelles et civiles?

4. L'ENCADREMENT NORMATIF

Depuis de nombreuses années déjà, des lois ont été édictées pour protéger les renseignements personnels et le droit à la vie privée des citoyens. Toutefois, le développement fulgurant de l'information et de la communication électroniques a fait en sorte que cette législation n'est pas toujours adaptée aux réalités nouvelles et qu'il est possible d'aller à l'encontre de l'esprit de la loi en cette matière. Des aménagements importants ont été faits aux lois existantes afin d'y inclure de nouvelles règles ou d'adapter les règles existantes. Le besoin se répète aujourd'hui avec l'émergence des technologies biométriques qui imposent de nouvelles législations ou l'adaptation de celles qui existent pour assurer la protection de la vie privée et des droits fondamentaux des citoyens.

À l'échelle canadienne, il n'existe pas encore de loi fédérale qui considère l'utilisation des biométries comme outils de collecte d'information et établisse les balises nécessaires en la matière, notamment en ce qui a trait à la protection de la vie privée et des renseignements personnels. Pour le moment, et de façon indirecte, œ sont la *Charte canadienne des droits et libertés,* le *Code criminel,* la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*, cette dernière en vigueur depuis janvier 2001, qui servent de garde-fou aux abus et aux dérives qui pourraient se produire.

À l'échelle québécoise, signalons la *Charte des droits et libertés de la personne* qui garantit à toute personne le droit au respect de sa vie privée. S'y ajoutent la *Loi œoncernant le cadre*

juridique des technologies de l'information qui répond en partie aux inquiétudes que soulève le recours à la biométrie, notamment les articles 44 et 45, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et, pour les entreprises du secteur privé, la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Il est important de reconnaître que des efforts sont réalisés sur le plan juridique pour accompagner l'évolution des technologies de l'information et de la communication, y compris leur ouverture récente sur les technologies biométriques. Toutefois, compte tenu des utilisations actuelles et potentielles de ces dernières, tout autant par l'État que par l'entreprise privée et même les particuliers, il importe de s'interroger sur la capacité des lois actuelles à contrer les dérives éventuelles et à assurer la population que ses droits fondamentaux seront protégés.

5. LE QUESTIONNEMENT ÉTHIQUE

Le tour d'horizon proposé dans le *Document de réflexion* de la Commission et le questionnement soulevé illustrent que l'utilisation de la biométrie à des fins de sécurité doit être l'objet de préoccupations de la part des citoyens et d'une réflexion éclairée de la part des gouvernements, entre autres en ce qui a trait à la protection des renseignements personnels et au respect de la vie privée. Mais d'autres questions se posent aussi, dans une société démocratique, sur le glissement éventuel vers un renversement du fardeau de la preuve – prouver son innocence plutôt que sa culpabilité – et vers la marginalisation de certains groupes en raison de leur origine ethnique et de leurs croyances. Une double interrogation apparaît fondamentale : le recours aux données biométriques constitue-t-il le moyen le plus adéquat pour contrer les problèmes de sécurité associés au terrorisme, au vol d'identité et à l'intrusion malfaisante dans des sites physiques ou informatiques? ses retombées possibles sur la démocratie, sur les libertés civiles, sur la protection des renseignements personnels, sur le respect de la vie privée, sur certains segments de la population sont-elles suffisamment prises en considération?

Toutefois, il importe de considérer que ces techniques peuvent aussi être perçues comme des techniques pouvant contribuer à une meilleure protection de la vie privée. Il y a donc là un paradoxe important. Dans les paragraphes qui suivent, en s'appuyant sur cette prémisse, la Commission propose le questionnement éthique suivant :

5.1 … sur le respect de la démocratie

De façon générale, la mise en place de systèmes biométriques soulève des inquiétudes sur la protection des libertés, de la vie privée et des droits fondamentaux des personnes, des valeurs qui sont représentatives des sociétés démocratiques. La biométrie est reconnue comme une technologie qui, par les mécanismes de surveillance qu'elle permet, donne un pouvoir important aux États et aux organisations dans le contrôle des personnes (citoyens ou employés). À la suite du 11 septembre, bon nombre des mesures de sécurité qui ont été mises en place ont eu pour effet de renforcer les pouvoirs des gouvernements et des systèmes judiciaire et policier, notamment pour leur permettre d'exiger des citoyens des informations à caractère personnel beaucoup plus détaillées qu'auparavant et d'y accéder à d'autres fins que celles pour lesquelles elles ont été initialement fournies.

Question : L'utilisation des technologies biométriques risque-t-elle de porter atteinte à la démocratie et de quelle façon? (enjeu du respect de la démocratie, enjeu de rationalité instrumentale)

5.2 …sur le renversement du fardeau de la preuve

Dans les sociétés de droit, toute personne bénéficie d'une présomption d'innocence face à la loi. Le recours à l'utilisation des technologies biométriques pour confirmer l'identité d'une personne risque de renverser ce principe juridique.

Question : Dans un contexte où contrôle et surveillance visent à créer un environnement sécuritaire au bénéfice de l'ensemble de la population, comment protéger l'*a priori* d'innocence? comment assurer les droits des victimes? (enjeu d'équité)

5.3 …sur la validité d'une donnée biométrique

L'interrogation qui précède sur le renversement du fardeau de la preuve soulève la question de la validité d'une donnée biométrique, de son caractère « authentique », advenant contestation de la part d'une personne qui en aurait été dépossédée. Comment une personne pourra-t-elle recouvrer son identité si ses propres données biométriques ne correspondent pas à celles enregistrées à son nom? En outre, dans un contexte judiciaire, par exemple, l'information stockée dans un système biométrique pourrait-elle éventuellement tenir lieu de preuve pour incriminer ou innocenter un prévenu, comme c'est déjà le cas pour l'ADN et les empreintes digitales?

Question : Faut-il mettre en place des mécanismes pour protéger les citoyens des erreurs qui pourraient se produire sur la foi de résultats fournis par un système biométrique? (enjeu d'équité et de justice, de respect de la personne)

5.4 … sur la protection des données personnelles : confidentialité et vie privée

La question de la protection des données personnelles est indissociable des systèmes biométriques, car les mesures biométriques sont considérées comme des renseignements confidentiels. C'est à ce titre qu'elles sont protégées par des mécanismes propres à assurer leur caractère confidentiel. Toutefois, en matière de conservation des données, certains experts en sécurité admettent que les bases de données centralisées constituent un risque en soi et peuvent exciter la convoitise des pirates informatiques; pour les données biométriques conservées sur un support portable, les possibilités de vol du support lui-même et de la capture d'information à l'insu des utilisateurs doivent être envisagées. Il faut également noter le risque qu'un État souhaite tirer profit de cette mine d'information à toutes sortes de fins, bénéfiques ou non pour la société dans son ensemble ou pour certains segments de la population particulièrement vulnérables. Enfin, la question des transferts transfrontaliers de l'information présenterait les incertitudes les plus inquiétantes.

Question : Les mécanismes actuels de protection des renseignements personnels permettent-ils d'en assurer pleinement la confidentialité et le respect de la vie privée? sont-ils adéquatement adaptés à l'émergence des technologies biométriques? d'autres mesures s'imposent-elles à cet égard? (enjeu de confidentialité et de respect de la vie privée, d'équité)

5.5 …sur le stockage et la gestion des données : accès, utilisation, divulgation

Contrairement à bien d'autres sociétés occidentales, le Québec peut s'appuyer sur un cadre législatif qui établit certaines balises en ce qui a trait aux banques de données biométriques. Toutefois, dans des situations où il n'existe aucune conservation de l'information recueillie en mémoire informatique ou sur support papier et quand la collecte de données biométriques n'a pas pour objet d'établir un lien entre une personne et un document, les lois en vigueur ne s'appliquent pas.

Question : Tous les éléments pertinents au stockage et à la gestion des bases de données biométriques sont-ils pris en compte dans la législation actuelle? et protègent-ils suffisamment l'information colligée contre toute utilisation malveillante? (enjeu de sécurité, d'équité et de confidentialité)

5.6 …sur la discrimination

Les données biométriques peuvent être qualifiées de « délicates » car certaines d'entre elles, outre l'ADN, peuvent révéler l'origine ethnique d'une personne (la reconnaissance faciale, par exemple) ou son état de santé (la lecture de l'iris, par exemple). Particulièrement sur le plan ethnique, ce sont des données qui peuvent éventuellement se prêter au « ciblage » de certaines catégories de personnes, notamment dans le contexte actuel de lutte au terrorisme. Sur ce plan, mais aussi sur d'autres aspects de l'information véhiculée par une donnée biométrique, il faut également considérer que des décisions concernant des personnes peuvent être prises de façon automatique par des systèmes informatisés, sur la seule base de l'information disponible. De telles décisions, prises à l'insu de la personne, à partir d'une information utilisée hors contexte et fondée sur des faits parfois incomplets, imprécis, non pertinents ou utiles, peuvent s'avérer préjudiciables à la personne concernée.

Question : Quelle peut-être l'ampleur des risques de discrimination associés à l'utilisation de systèmes biométriques à des fins de sécurité? de quelle façon contrer ces risques? (enjeu d'équité)

5.7 …sur le manque de transparence : le consentement

L'article 44 de la *Loi concernant le cadre juridique des technologies de l'information* stipule que toute vérification ou confirmation de l'identité d'une personne au moyen de mesures biométriques ne peut se faire sans son « consentement exprès ». Et il est interdit à un organisme public de recueillir une donnée biométrique si cette donnée n'est pas nécessaire à l'exercice de ses fonctions ou à la mise en œuvre d'un programme dont il a la gestion. L'obtention d'un consentement ne permet pas de contourner cette interdiction. Il en va de même pour une entreprise du secteur privé qui ne peut recueillir que les seules données qui sont nécessaires à l'objet du dossier constitué sur une personne. Or, nombre de données biométriques peuvent être recueillies à l'insu de la personne concernée (les empreintes digitales, l'ADN, la reconnaissance faciale, la démarche ou la dynamique de frappe sur un clavier, par exemple).

Question : Comment s'assurer que l'obligation de consentement est respectée, notamment dans le cas des technologies biométriques qui peuvent être utilisées à l'insu de la personne? comment éviter que le libre choix ainsi autorisé par la loi n'ait pas de conséquences négatives pour la personne qui s'en prévaut? (enjeu de la transparence et du libre choix)

5.8 … sur le respect des finalités

Conformément aux lois en vigueur, la finalité d'utilisation des données biométriques doit être explicite, légitime et clairement définie et aucune information révélée par ces données ne peut être utilisée à quelque autre fin que ce soit. Toutefois, compte tenu de la somme d'information qui peut être extraite d'une base de données spécifique ou à partir d'un croisement de plusieurs bases de données (biométriques et autres), « le risque d'accroître les possibilités de réutilisation de ces données par des tiers comme éléments de comparaison et de recherche dans le cadre de leurs propres activités, sans que cet objectif ait été envisagé initialement » ne peut être occulté, souligne la Commission européenne.

Question : Comment s'assurer que les finalités énoncées sont respectées et qu'aucun détournement ne puisse se produire au détriment de certaines personnes ou groupes de personnes vulnérables? (enjeu de confiance, de transparence, de respect des personnes, d'équité)

5.9 …sur la proportionnalité des moyens

Les données biométriques et les systèmes biométriques mis en place ont pour but l'identification et l'authentification (la vérification) des personnes pour assurer la sécurité de la population (sur le plan national et international) et des infrastructures matérielles ou informatiques. Il semble opportun de signaler que des techniques de « surveillance de masse », qui misent le plus souvent sur la reconnaissance faciale, sont de plus en plus utilisées par les responsables de l'ordre public qui espèrent ainsi repérer des personnes ou des agissements suspects, et prévenir la criminalité ou les actes terroristes. Toute la population est ainsi susceptible d'être filmée à son insu, pour des motifs qui peuvent sembler louables. En ce qui a trait aux systèmes biométriques mis en place pour les voyageurs qui utilisent l'avion, et le train dans certains cas, ils ont pour but de contrer l'entrée illicite d'éventuels terroristes. Toutefois, les terroristes peuvent aussi être des citoyens de plein droit du pays qui effectue le contrôle et ceux qui ne le sont pas savent généralement comment contourner les mesures de contrôle qui sont instaurées. Il convient aussi de s'interroger sur la proportionnalité des mesures de contrôle biométrique utilisées sur les lieux de travail en fonction des objectifs poursuivis et sur les solutions de rechange qui pourraient être envisagées.

Question : Les mesures biométriques constituent-elles une solution souhaitable et appropriée pour répondre aux besoins actuels de contrer le terrorisme, de combattre la criminalité sur le territoire et de protéger les infrastructures matérielles et informatiques contre toute intrusion malveillante? d'autres moyens moins intrusifs pourraient-ils s'avérer tout aussi efficaces? (enjeu de proportionnalité des moyens et d'équité)

5.10 … sur l'instrumentalisation du corps humain

Se fondant sur la définition suivante de l'instrumentalisation du corps humain : « toute conception qui réduit la vie à des composantes physico-chimiques et considère que les processus vitaux ne sont pas différents des processus physiques », la Commission estime qu'il faut considérer ce risque en ce qui concerne le recours aux technologies biométriques et que cette préoccupation doit faire partie du questionnement éthique.

Question : Le recours aux technologies biométriques comporte-t-il un risque d'instrumentalisation du corps humain et de quelle nature serait ce risque? (enjeu du respect de la dignité humaine)

5.11 … sur les effets sur la santé

En ce qui a trait aux effets sur la santé, les technologies qui soulèvent des questions à cet égard sont celles qui concernent l'œil (iris et rétine) et celles qui comportent un contact physique direct avec un capteur biométrique (empreintes digitales et paume de la main). Dans le premier cas, les craintes concernent les lésions que les rayons infrarouges pourraient causer à l'œil; dans l'état actuel des choses, la lecture rétinienne n'est pas encore suffisamment développée pour que des problèmes aient été détectés; quant à la reconnaissance de l'iris, aucun problème n'aurait été rapporté jusqu'à présent, malgré le caractère assez répandu de cette technologie. En ce qui concerne les contacts physiques, les craintes sont associées à la contamination possible par le biais de la présence de germes ou de bactéries sur le capteur; il est généralement reconnu que ces appareils exigent des mesures spécifiques (nettoyage aux rayons ultraviolets, par exemple)

pour contrer le problème. Le questionnement à cet égard est très peu présent dans la documentation colligée sur le sujet.

Question : Peut-il y avoir des effets nocifs pour la santé qui résultent de l'utilisation de certaines applications de la biométrie? de quelle nature pourraient-ils être? des recherches en ce sens sont-elles entreprises? (enjeu de protection de la santé)

5.12 …sur l'encadrement normatif

Le Québec dispose d'une réglementation qui peut tenir compte de la mise en place et de l'utilisation de la biométrie. Le Canada, pour sa part, souhaite une approche législative uniforme qui pourrait utiliser les lois en vigueur au Québec et en Ontario comme point de départ. Par ailleurs, si le Canada dispose d'un régime national de protection de la vie privée qui repose sur le code de l'OCDE, bien d'autres pays n'ont encore aucune loi à cet effet, ce qui soulève la question de la réciprocité dans les échanges d'information.

Question : Y a-t-il un risque de gain ou de perte pour la population québécoise? À quelles fins faut-il également rechercher une harmonisation internationale en la matière? Qu'en sera-t-il de la réciprocité dans les échanges de renseignements personnels, le cas échéant, et dans quelle mesure les règles en vigueur au Canada et au Québec seront-elles respectées à l'étranger? (enjeu de respect de la vie privée et de confidentialité)

5.13 … sur les dérives possibles

Les dérives possibles d'une offre croissante de systèmes biométriques sur le marché ne sont pas négligeables. De tels systèmes sont déjà offerts et utilisés par différents niveaux de gouvernement tout comme par l'entreprise privée. Outre des objectifs de protection contre le terrorisme et contre la criminalité, leur utilisation pourra répondre à toutes sortes de finalités, plus ou moins légitimes dont la surveillance au travail ou dans les maisons privées, le contrôle des entrées et des sorties du personnel, l'évaluation de l'état émotionnel de certaines personnes (données reposant sur la chaleur dégagée, par exemple), ou de leur état de santé (ADN, réseaux veineux, rétine, etc.) ne constituent que quelques exemples.

Question : À quel point les dérives possibles de l'utilisation de systèmes biométriques par les secteurs public et privé sont-elles prises en considération par la législation actuelle? chaque personne est-elle suffisamment protégée contre les abus possibles que peut entraîner le recours aux données biométriques dans sa vie personnelle et professionnelle. (enjeu de responsabilité morale)

CONCLUSION

Les questions que la Commission se pose à la suite de la préparation de son document de réflexion pourraient en fait se résumer de la façon suivante : *Dans le but d'assurer la sécurité internationale et nationale, notamment au moyen de l'utilisation des données biométriques, les fondements de la démocratie et les droits des citoyens sont-ils encore respectés? L'objectif de sécurité représente-t-il une situation où la fin justifie les moyens?*

Avant de proposer aux décideurs publics et institutionnels un avis et des recommandations sur les enjeux éthiques de la biométrie, la Commission soumet au débat public un état de situation sur le sujet et le questionnement éthique qui en résulte. Afin d'alimenter sa réflexion dans la préparation de cet avis, elle souhaite entendre les poins de vue d'experts de divers horizons disciplinaires et de spécialistes de l'éthique sur le questionnement qu'elle a soulevé. Mais elle souhaite également

entendre ce qu'en pense la population de façon à émettre une opinion et des recommandations qui soient bien ancrées dans la réalité sociale et citoyenne.

En marge du forum, il est aussi possible à toute personne ou association qui le désire de participer à la consultation en faisant parvenir ses commentaires ou réactions au questionnement éthique du document de consultation de la CEST au plus tard le 30 novembre 2005, selon l'une ou l'autre des modalités suivantes :

- par courriel : ethique@ethique.gouv.qc.ca
- par télécopieur : (418) 646-0920
- par courrier postal : Commission de l'éthique
  de la science et de la technologie
  1200, route de l'Église
  3e étage, Bureau 3.45
  Sainte-Foy (Québec) G1V 4Z2

ACTIVITÉS DE CONSULTATION DE LA COMMISSION

ET REMERCIEMENTS

Experts rencontrés par la CEST pour la préparation de son document de réflexion*:*

- ***Thème de discussion : Aspects techniques de la biométrie et enjeux éthiques***

M. Bernard Dionne (aspects techniques) et **M^me^ Èvelyne Racette** (enjeux éthiques), professionnels de recherche, ministère des Relations avec les citoyens et de l'Immigration

- ***Thème de discussion : La construction de la peur et le catastrophisme***

M. Jacques de Guise, spécialiste de la communication, professeur retraité de l'Université Laval

M^me^ Hélène Denis, spécialiste de la gestion du risque, professeure retraitée de l'École Polytechnique de Montréal

- ***Thème de discussion : Terrorisme, sécurité, démocratie***

M. Benoît Gagnon, chercheur, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal

M. Albert Legault, titulaire de la Chaire de recherche du Canada en relations internationales, Université du Québec à Montréal

M. Kevin McGarr, directeur de la recherche, Administration canadienne de la sécurité du transport aérien (ACSTA), gouvernement du Canada

En avril 2005, les personnes suivantes ont accepté de procéder à une lecture critique d'une première version du document de réflexion de la Commission :

M. Max Chassé, spécialiste de la biométrie, Conseil du trésor (Québec)

M^me^ Jocelyne Couture, directrice des études des cycles supérieurs, département de philosophie, Université du Québec à Montréal

M. Raymond d'Aoust, commissaire adjoint, Commissariat à la protection de la vie privée (Canada)

M. Jérôme Gagnon, conseiller, Direction de la prévention et de la lutte contre la criminalité, ministère de la Sécurité publique (Québec)

M. Albert Legault, titulaire de la Chaire de recherche du Canada en relations internationales, Université du Québec à Montréal

M. Stéphane Leman-Langlois, criminologue, École de criminologie, Université de Montréal

M. Kevin McGarr, directeur de la recherche, Administration canadienne de la sécurité du transport aérien (ACSTA), gouvernement du Canada

M. Pierre Patenaude, professeur titulaire, Faculté de droit, Université de Sherbrooke

La Commission remercie toutes ces personnes. Par leur collaboration, elles ont contribué à l'enrichissement de son document de réflexion.

Commission de l'éthique de la science et de la technologie
Québec

LES PUBLICATIONS DE LA COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

La liste qui suit mentionne toutes les publications parues depuis 2002. Il est possible de les consulter et de les télécharger en accédant au site Web de la Commission de l'éthique de la science et de la technologie (www.ethique.gouv.qc.ca). Des résumés en français, en anglais et en espagnol accompagnent chacun des avis dans le site.

À moins d'indication contraire, les documents sont également disponibles en version imprimée et peuvent être obtenus en adressant une demande à :

Commission de l'éthique de la science et de la technologie
1200, route de l'Église, bureau 3.45
Sainte-Foy QC G1V 4Z2
Téléphone : (418) 528-0965
Télécopieur : (418) 646-0920
Courriel : ethique@ethique.gouv.qc.ca
ou lauraine.berard@cst.gouv.qc.ca

AVIS

Le don et la transplantation d'organes : dilemmes éthiques en contexte de pénurie
Novembre 2004, 142 p.; ISBN 2-550-43415-3

Organ Donation and Transplantation : Ethical Dilemmas Due to Shortage
November 2004, 145p.; ISBN 2-550-43415-3 (fichier pdf seulement)

Pour une gestion éthique des OGM
Décembre 2003, 144 p.; ISBN 2-550-41769-6

Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable
Février 2003, 97 p.; ISBN 2-550-40365-7

DOCUMENT DE RÉFLEXION

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques
Juin 2005, 87p.; ISBN 2-550-44634-8

MÉMOIRE

Les nouveaux enjeux de la sécurité alimentaire au Québec
Janvier 2004, 40 p.

ÉTUDES ET RECHERCHES

Documents complémentaires à l'avis *Pour une gestion éthique des OGM*

Disponibles uniquement sur le site Web (www.ethique.gouv.qc.ca/fr/publications.html)

Rapport de recherche sur la couverture médiatique au Québec en matière d'alimentation et d'OGM
Juin 2003, 29 p.
Par Richard Lair et Alain Létourneau

Financement de la recherche dans le secteur des biotechnologies : le cas des OGM
Janvier 2003, 23 p.
Par Guillaume Lavallée

Les représentations véhiculées dans la culture amérindienne du Québec en ce qui a trait à l'alimentation, aux organismes génétiquement modifiés (OGM) et aux transformations que l'humain peut apporter à la nature
Décembre 2002, 49 p.
Par Jose Lopez Arellano

Est-il possible de faire... sans la transgénèse?
Novembre 2002, 13 p.
Par Jean-François Sénéchal

Le christianisme et les OGM
Novembre 2002, 13 p.
Par André Beauchamp

Cuisine de Dieu – Aliments profanes. Prohibitions alimentaires du judaïsme, organismes génétiquement modifiés et enjeux éthiques
Octobre 2002, 52 p.
Par Michaël Elbaz et Ruth Murbach

Le bouddhisme et les OGM
Septembre 2002, 33 p.
Par Charles-Anica Endo

L'Islam et les OGM
Septembre 2002, 35 p.
Par Ali Maarabouni

Les modifications génétiques chez les microorganismes
Août 2002, 17 p.
Par Isabelle Boucher

OGM végétaux
Août 2002, 40 p.
Par Éric Dion

Vue d'ensemble des techniques usuelles en transgénèse animale
Août 2002, 9 p.
Par Jean-François Sénéchal

Documents complémentaires à l'avis *Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable*
Disponibles uniquement sur le site Web (www.ethique.gouv.qc.ca/fr/publications.html)

Les banques d'information génétique dans le monde : aperçu de la situation
Janvier 2003, 32 p.
Par David Boucher et Emmanuelle Trottier

Le consentement libre et éclairé : un paradigme révolu en matière de recherche génétique sur les populations?
Décembre 2002, 18 p.
Par Dany Joncas

Les banques de données génétiques et le droit étranger
Octobre 2002, 30 p.
Par Dany Joncas

RAPPORT ANNUEL

Rapport d'activité 2001-2003 et perspectives d'avenir
Octobre 2003, 30 p.; ISBN 2-550-41684-8 et ISSN 1708-8534

BROCHURE

Les banques d'information génétique : «C'est BIG!»
Mars 2004, 27 p.; ISBN 2-550-42074-8
Par Luc Dupont

CONSULTATION

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques
Document de consultation
Juin 2005, 18p.; ISBN 2-550-44626-7

Rapport de consultation sur les enjeux éthiques du don et de la transplantation d'organes. Résultats des entrevues de groupes et du mini-sondage réalisé dans le cade de l'Enquête Stamédia printemps 2004
Novembre 2004, 94 p.; ISBN 2-550-43416-1

Les enjeux éthiques du don et de la transplantation d'organes
Document de consultation
Mai 2004, 41 p.; ISBN 2-550-42564-2

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques est un document de consultation que la Commission de l'éthique de la science et de la technologie soumet au débat public. Considérant l'intensification des mesures de contrôle et la disponibilité croissante de moyens techniques fondés sur l'acquisition de données personnelles et l'utilisation de traits personnels – des données biométriques – pour établir ou contrôler l'identité d'une personne, la Commission estime urgent de s'interroger sur les enjeux éthiques que la question soulève et d'en débattre publiquement.

D'entrée de jeu, la Commission souligne l'importance de la sécurité pour l'être humain et pour les cités. Elle fait ensuite le point sur les aspects techniques de la biométrie, sur ses champs d'application – lutte au terrorisme et à la criminalité reliée au vol d'identité, contrôle de l'accès à des sites physiques ou virtuels – et sur les encadrements normatifs (lois, règlements ou autres) qui permettent de baliser le domaine, pour ensuite signaler les enjeux éthiques que soulève l'application de la technologie biométrique dans une société pluraliste et démocratique. Ces enjeux ne sont cependant abordés que succinctement dans le présent document; la consultation que mène la Commission sur le sujet, tant auprès d'experts qu'auprès de la population, lui permettra d'amorcer la préparation d'un avis sur ce thème à l'intention des décideurs politiques et institutionnels.

Ce document de consultation de la Commission, ainsi qu'un document de réflexion plus détaillé, sont disponibles en fichiers électroniques à l'adresse suivante : **www.ethique.gouv.qc.ca**

*La **mission** de la CEST consiste, d'une part, à informer, sensibiliser, recevoir des opinions, susciter la réflexion et organiser des débats sur les enjeux éthiques du développement de la science et de la technologie, et, d'autre part, à proposer des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.*

Commission
de l'éthique
de la science
et de la technologie
Québec