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

1200, route de l'Église
3e étage, bureau 3.45
Québec (Québec)
G1V 4Z2
www.ethique.gouv.qc.ca

En soutien à la réalisation de l'avis

Coordination et supervision

Diane Duquet et Nicole Beaudry

Secrétaire de réunion

David Boucher

Recherche et rédaction

David Boucher et Diane Duquet

Soutien technique

Secrétariat

Annie St-Hilaire

Documentation

Monique Blouin et Annie Lachance

Communication et supervision de l'édition

Guillaume Huet

Révision linguistique

Le Graphe

Conception de la page couverture

Création Sylvain Vallières inc.

Conception et mise en pages

Éditions MultiMondes

Impression

Imprimerie Le Laurentien

Avis adopté à la 34e réunion de la Commission de l'éthique de la science et de la technologie le 12 février 2008

Dépôt légal : 2008
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN 978-2-550-52239-3

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

Les membres du Comité de travail

Président

Benoît Gagnon
Chercheur associé
Chaire de recherche du Canada en sécurité, identité et technologie
Doctorant à l'Université de Montréal

Membres

Frédéric Abraham
Doctorant en philosophie
Université du Québec à Trois-Rivières

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

Me Édith Deleury
Présidente de la CEST
Faculté de droit
Université Laval

Benoît Dupont
Titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie
Professeur
École de criminologie
Université de Montréal

Frédérick Gaudreau, lt
Coordonnateur
Module de la cybersurveillance et de la vigie
Sûreté du Québec

Stéphane Leman-Langlois
Chercheur régulier
Centre international de criminologie comparée (CICC)
Professeur
École de criminologie
Université de Montréal

Me Danielle Parent
Directrice des affaires juridiques
Bureau du Commissaire au lobbyisme du Québec

Me Marie-Claude Prémont
Professeure de droit
École nationale d'administration publique (ÉNAP)

Serge Trudel
Directeur dossier de l'Accès à l'information/éthique
Association canadienne de la sécurité (CANASA)

Daniel Marc Weinstock
Titulaire de la Chaire de recherche du Canada en éthique et en philosophie politique
Professeur
Département de philosophie
Université de Montréal

Membre observateur

Raymond D'Aoust
Commissaire adjoint
Commissariat à la protection de la vie privée du Canada

Du secrétariat de la Commission

Me Nicole Beaudry, coordonnatrice de la CEST
David Boucher, conseiller en éthique et secrétaire du comité de travail

Table des matières

Liste des sigles et acronymes

AAPI :	Association sur l'accès et la protection de l'information
ADN :	Acide désoxyribonucléique
CAI :	Commission d'accès à l'information (Québec)
CANASA :	Association canadienne de la sécurité
CCNE :	Comité consultatif national d'éthique pour les sciences de la vie et de la santé (France)
CNIL :	Commission nationale de l'informatique et des libertés (France)
IRF :	Identification par radiofréquence
NTSC :	Nouvelles technologies de surveillance et de contrôle
OCDE :	Organisation de coopération et de développement économiques
ONU :	Organisation des Nations Unies

Résumé et recommandations

La surveillance de masse peut être considérée comme un trait caractéristique des sociétés modernes. Son importance n'a d'égal que les moyens mis en place pour amasser des renseignements. Parmi ces moyens, les nouvelles technologies de surveillance et de contrôle (NTSC) et surtout les manières de les déployer soulèvent des enjeux éthiques. Aussi la Commission de l'éthique de la science et de la technologie s'est-elle donné le mandat de formuler un avis sur des technologies pouvant servir à la surveillance de masse à des fins de sécurité : les systèmes biométriques, la vidéosurveillance et l'identification par radiofréquence (IRF).

La Commission tient à préciser qu'elle voulait traiter des NTSC sous l'angle de leurs applications à des fins de sécurité, ce qui excluait notamment les fins de surveillance sur les lieux de travail, les fins associées à la santé et les applications liées à la gestion des inventaires. Mais qu'est-ce que la sécurité ? Poser la question met déjà en évidence la complexité du concept. En effet, non seulement le terme renvoie à différentes notions, notamment sur le plan sociologique, mais son interprétation varie en fonction des langues, des discours, des approches et de l'histoire.

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, et surtout depuis les événements du 11 septembre 2001, les paramètres du danger et de la sécurité semblent entièrement nouveaux et paraissent exiger l'adoption de mesures également nouvelles sur le plan tant technique que politique. Les NTSC sont l'une de ces nouvelles mesures.

Histoire de camper sa réflexion dans un contexte social, politique et éthique élargi, la Commission s'est interrogée dans un premier temps sur les liens susceptibles d'exister entre le déploiement des NTSC et certains phénomènes comme le sentiment d'insécurité par rapport à la criminalité et l'importance grandissante des notions de risque et de surveillance.

Tout d'abord, la Commission désirait y voir plus clair quant au sentiment d'insécurité auquel il est souvent fait référence dans les médias. Il s'avère en fait que le sentiment que les gens ont de leur propre sécurité dépend de plusieurs facteurs et qu'il peut être influencé par différents acteurs. Par conséquent, il s'agit d'une réalité plutôt difficile à cerner. Pour tenter de mieux évaluer l'ampleur réelle du sentiment d'insécurité, la Commission a examiné plusieurs enquêtes et sondages sur le sujet. Selon les données analysées il peut être conclu que les Canadiens et les Québécois se sentent en sécurité. La place qu'occupe dans les médias la couverture des actes criminels et terroristes ne refléterait donc aucunement les préoccupations de la population interrogée. De plus, une forte peur du crime viendrait en contradiction avec les statistiques sur la criminalité, du moins au Canada, qui font état d'un recul de la criminalité depuis quelques années.

Une société qui est alimentée, volontairement ou non, par une certaine insécurité est plus encline à exprimer un besoin constant d'informations pour évaluer et gérer les risques et les dangers qui la guettent. Plusieurs penseurs estiment que le fait d'être obsédé par les risques, les menaces et les dangers est un symptôme de l'insécurité qui affecte une société. C'est d'ailleurs pourquoi des auteurs, comme le sociologue Ulrich Beck, qualifient ces sociétés de sociétés du risque. Parmi les caractéristiques des sociétés du risque à mentionner, le besoin d'information de ses gestionnaires, mais aussi des citoyens, est particulièrement pertinent dans le cadre de l'avis de la Commission. Car, selon les théoriciens de la société du risque, plus l'information dont les personnes disposent est grande, plus ils sont en mesure de calculer, d'analyser et de gérer les risques dans l'espoir de les réduire, voire de les éliminer. Lorsque ce principe est appliqué au domaine de la sécurité, il devient évident pour la Commission que les NTSC constituent un puissant moyen de collecte d'informations servant à contrecarrer les menaces à la sécurité et à réduire la criminalité. Sans affirmer que l'attrait pour les NTSC se

réduit à ces seules logiques, la Commission n'en estime pas moins qu'il s'agit là d'un des moteurs derrière le déploiement des NTSC à des fins de sécurité.

La collecte d'informations est, par conséquent, absolument vitale pour la société du risque. Ces informations sont obtenues, entre autres, par la surveillance. Mais la surveillance ne constitue pas un phénomène nouveau, car elle n'a pas attendu l'avènement d'une société du risque ou de technologies raffinées pour se manifester. La surveillance est reconnue comme partie intégrante de toutes les sociétés humaines depuis des temps immémoriaux, puisque le simple acte de socialisation serait impensable sans la surveillance exercée par les adultes. Récemment, et surtout en réaction aux événements du 11 septembre 2001, un changement de cap est observable dans les méthodes de collecte de renseignements. L'objet de la surveillance ne se limite plus à quelques segments de la population déjà considérés comme « à risque ». C'est maintenant la population en général qui est placée sous surveillance afin de cibler des interventions vers les personnes jugées à risque ou qui posent des risques pour d'autres personnes.

Ce n'est pas vraiment l'apparition imminente d'un *Big Brother* qui inquiète la Commission. En fait, c'est l'avènement de nombreux *Small Brothers*, c'est-à-dire de plusieurs organismes et personnes qui, à titre privé, se mettent à faire de la surveillance à des fins de sécurité, qui est préoccupant. Ce genre de surveillance qui ne respecte pas nécessairement toujours les lignes directrices et les bonnes pratiques en la matière risque d'échapper totalement au contrôle de l'État.

Prenant appui sur ces éléments de contexte, la Commission définit ensuite le cadre éthique dans lequel elle s'inscrit pour porter un regard éthique sur les NTSC. Au regard des valeurs, la Commission souligne son attachement aux valeurs fondamentales au sein des sociétés démocratiques et plus particulièrement à la valeur d'autonomie. Dans les sociétés démocratiques libérales, cette valeur joue en effet un rôle central. L'autonomie est cette valeur qui permet aux personnes de mener et d'accomplir un projet de vie comme bon leur semble, dans les limites imposées par les droits et libertés des autres personnes. Dans le présent avis, elle est conçue comme l'expression de la liberté des citoyens des sociétés démocratiques, notamment par rapport au regard, qui peut parfois être intrusif, de l'État et d'autres organisations. En outre, la Commission estime que plus les citoyens participeront à l'élaboration, à la mise en place et au suivi des balises entourant le déploiement des NTSC, plus ce processus sera conforme à l'idéal démocratique et respectera la valeur d'autonomie.

Cette volonté de privilégier l'autonomie des personnes dans les démocraties libérales se matérialise plus concrètement par l'attachement à toute une constellation de valeurs fondamentales. Bien que ces valeurs puissent, dans certains cas précis, entrer en conflit, il convient de reconnaître qu'elles ont un point commun. Elles rendent possibles l'autonomie et, partant, la vie démocratique. Parmi cet ensemble de valeurs, la Commission a retenu celles qu'elle estimait les plus concernées par le déploiement des NTSC, c'est-à-dire la sécurité, la liberté, la vie privée, la transparence, la justice et l'égalité. La Commission met ainsi l'accent sur le fait que le recours aux NTSC ne doit jamais faire abstraction de son objectif primordial : protéger les sociétés démocratiques contre les risques d'atteinte à leurs valeurs fondamentales. En cherchant à assurer une trop grande sécurité, les moyens de surveillance peuvent en effet menacer le respect des valeurs fondamentales des sociétés démocratiques. Le but de la Commission, avec le présent avis, est donc de viser un juste équilibre entre la sécurité et les droits et libertés individuels dans la protection des valeurs fondamentales des sociétés démocratiques.

Sur le plan technique, la Commission fournit une description détaillée des trois NTSC qui ont retenu son attention.

Un **système biométrique** permet d'identifier une personne ou vérifie l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)[1] ». Les applications des systèmes biométriques sont encore plutôt rares.

1. Définition de la Commission nationale de l'informatique et des libertés (CNIL – France), rapportée dans OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, France, Assemblée nationale, 2003, p. 8.

La **vidéosurveillance** consiste en la surveillance à distance de lieux publics ou privés, à l'aide de caméras le plus souvent motorisées, qui transmettent les images saisies à un équipement de contrôle qui les reproduit sur un écran. Dans ce cas, il s'agit d'une technologie de surveillance et de contrôle beaucoup plus répandue et familière. Il est toutefois moins certain que les plus récentes avancées technologiques en la matière, comme la numérisation et le couplage avec des logiciels de reconnaissance faciale, soient aussi connues.

L'**identification par radiofréquence** (IRF ou RFID), sans être véritablement une nouvelle technologie, trouve à l'heure actuelle des applications surprenantes, et cela, dans divers domaines. Deux composantes principales rendent l'IRF possible. Tout d'abord, une puce dotée « d'un circuit électronique qui stocke des données et une antenne qui communique les données au moyen d'ondes radio[2] ». Cette puce communique avec un lecteur, lequel possède « une antenne et un démodulateur qui traduit l'information analogique […] en données numériques. L'information numérique peut alors être traitée par un ordinateur.[3] » En matière de sécurité, l'insertion de puces contenant des renseignements personnels ou d'autres informations (la nationalité, le sexe, la date de naissance, etc.) dans les documents d'identité et les cartes d'accès est la principale application de l'IRF. Pouvant être lues à distance, ces puces permettraient de suivre des personnes à la trace et de sécuriser des documents afin d'éviter la fraude et le vol d'identité.

Le déploiement des NTSC soulève plusieurs enjeux éthiques. La Commission a retenu quelques-uns d'entre eux pour en faire une analyse plus approfondie.

L'évaluation de la pertinence, de l'efficacité et de la fiabilité des NTSC

Pour assurer la légitimité de leur déploiement, la Commission estime que les nouvelles technologies de surveillance et de contrôle doivent être pertinentes, efficaces et fiables. Le critère de pertinence consiste à savoir si les NTSC s'avèrent le meilleur moyen pour répondre au besoin reconnu en matière de sécurité. Ainsi, d'autres moyens moins intrusifs sur le plan de la vie privée devraient être privilégiés. Pour que les NTSC soient efficaces, il faut que les résultats obtenus par leur déploiement correspondent aux visées d'origine. De plus, les NTSC doivent être fiables, c'est-à-dire qu'il faut éviter que leur fonctionnement ne soulève plus de problèmes qu'elles n'apportent de solutions. Pour être en mesure de justifier leur déploiement, il faudrait que les NTSC atteignent un niveau plus élevé de pertinence, d'efficacité et de fiabilité. La Commission estime également nécessaire de rappeler l'importance de déployer des technologies efficaces et fiables afin d'éviter de causer des préjudices à des personnes innocentes. Ces questions, bien qu'elles soient d'ordre plus technique, appellent des réponses dans lesquelles la valeur de transparence vis-à-vis la population occupe une place prépondérante. L'évaluation de l'efficacité des NTSC doit être aussi transparente que possible afin de permettre aux citoyens d'avoir l'heure juste à ce sujet. La Commission désire aussi mettre en garde contre le déploiement de technologies perçues comme fiables et qui contribueraient à répandre un faux sentiment de sécurité dans la population.

La proportionnalité de la réponse à l'insécurité

La Commission est préoccupée par l'ampleur que pourrait prendre un déploiement des NTSC qui se ferait l'écho d'une demande insatiable de sécurité. La mise en place de NTSC doit tenir compte des enjeux éthiques en la matière et chercher à atteindre un niveau de sécurité jugé acceptable, sans verser dans la surenchère sécuritaire. Il y a donc des ponts à établir entre les divers acteurs du milieu et la population afin d'en arriver à des consensus sur le sujet.

Avec le Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE), la Commission estime que la notion de proportionnalité des moyens doit être prise en considération, non seulement dans le cadre des systèmes biométriques, mais dans le déploiement des NTSC en général. Mettre en place des moyens de surveillance trop intrusifs sur le plan de la vie privée compte tenu des fins visées et du contexte, tout comme intégrer des données personnelles au-delà de ce qui est

2. GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU PARLEMENT EUROPÉEN ET DU CONSEIL, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, Bruxelles, 2005, p. 3 et 4. [http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf].
3. *Ibid.*

nécessaire à la finalité déclarée, ne serait pas acceptable sur le plan éthique. Aussi la Commission invite-t-elle les décideurs politiques et privés à procéder à une évaluation et à une interprétation nuancées et lucides des besoins en matière de NTSC à des fins de sécurité.

Il est primordial que l'évaluation du rapport entre la fiabilité technique, la proportionnalité de la réponse à l'insécurité et le degré d'intrusion dans la vie privée soit faite pour chaque projet de déploiement de NTSC. Il apparaît qu'une telle évaluation serait à même de permettre un regard éthique sur les finalités pour lesquelles les NTSC sont concrètement mises en œuvre. Une telle procédure serait inédite et elle aurait pour avantage indéniable de positionner le Québec comme un meneur sur le plan de l'évaluation éthique des utilisations de ce type de technologies.

Par ailleurs, au cœur de l'évaluation de la proportionnalité de la réponse à l'insécurité se trouvent des acteurs trop souvent ignorés par les décideurs publics et privés : les fournisseurs et les installateurs de NTSC. Ces acteurs se situent sur la première ligne en ceci qu'ils doivent assurer les besoins d'organisations publiques et privées et de citoyens en matière de sécurité sur le plan technique. En plus d'être en mesure de bien conseiller leurs clients en matière de NTSC, ces acteurs doivent pouvoir répondre à cette question : Quelle technologie conviendrait pour assurer un degré de sécurité donné ? En d'autres mots, quel système de sécurité est-il recommandé d'installer en fonction du degré de sécurité qu'il faut assurer ? Les fournisseurs et les installateurs sont les premiers confrontés aux enjeux éthiques mentionnés par la Commission. Aussi est-il nécessaire qu'ils soient sensibilisés à ces questions pour que le déploiement des NTSC se fasse en accord avec les valeurs privilégiées. La question centrale semble être de savoir comment parvenir à une proportionnalité dans la réponse à l'insécurité dans un contexte de marché en croissance très rapide et où la logique du profit l'emporte souvent sur la logique éthique. De telles considérations invitent à une réflexion approfondie sur la régulation des NTSC. Or, de récents développements sur le plan législatif permettraient de diffuser le fruit de cette réflexion parmi les acteurs du milieu.

Au Québec, la nouvelle Loi sur la sécurité privée encadre notamment « les activités reliées aux systèmes électroniques de sécurité, soit l'installation, la réparation, l'entretien et la surveillance continue à distance de systèmes d'alarme contre le vol ou l'intrusion, de systèmes de surveillance vidéo ou de systèmes de contrôle d'accès, à l'exception d'un système sur un véhicule routier […][4] ». La Loi précise entre autres que le futur Bureau de la sécurité privée dispensera de la formation aux représentants des titulaires de permis d'agence et que le gouvernement pourra, par règlement, déterminer quelle est la formation nécessaire pour l'utilisation d'équipement ou décider de la formation à exiger pour la délivrance d'un permis d'agent[5]. Cette formation devrait prévoir un volet obligatoire sur les enjeux éthiques. C'est pourquoi :

la Commission recommande que la formation dispensée par le Bureau de la sécurité privée aux représentants des titulaires de permis d'agence inclue un volet éthique obligatoire qui s'inspirera des enjeux éthiques soulevés dans le présent avis et que le gouvernement, conformément à la Loi sur la sécurité privée, adopte la réglementation nécessaire pour que la formation exigée pour la délivrance d'un permis d'agent prévoie également un tel volet éthique.

L'acceptabilité sociale

Il est difficile de déterminer le véritable niveau d'acceptabilité sociale du déploiement des NTSC. Une meilleure connaissance des perceptions et des opinions de la population en cette matière contribuerait certainement à y voir plus clair. Il est important que soient mieux connues les perspectives des citoyens à l'égard des NTSC. Il apparaît primordial de donner la parole à celles et ceux qui seront placés sous surveillance afin de favoriser un déploiement acceptable pour la société et accepté par elle.

En considérant la popularité actuelle des gouvernements qui font de la sécurité leur cheval de bataille et à la lumière des résultats de sondages et d'enquêtes sur l'acceptation des NTSC par la population, il semble que le déploiement des NTSC ne soit pas contraire à la volonté populaire. La Commission s'interroge toutefois sur le niveau de connaissance du public en matière de biométrie, de vidéosurveillance et d'identification par radiofréquence (IRF). Aussi toute forme de consultation sur les NTSC doit-elle faire une place importante à la population en général et chercher d'abord et avant tout à recueillir des opinions éclairées.

4. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 1.
5. L.R.Q., chapitre S-3.5, 2006, c. 23, a. 41, 111 et 112.

Le consentement

La plupart du temps, il est tout simplement impossible pour les personnes surveillées de consentir à ce qu'il en soit ainsi. En fait, le consentement libre et éclairé, sur une base individuelle, n'est tout simplement pas un concept opérationnel lorsque vient le temps de l'appliquer aux NTSC. Cela ne signifie pas pour autant qu'un tel état de fait ne soulève pas de questions d'ordre éthique, au contraire.

Des données biométriques peuvent en effet être recueillies à l'insu des personnes, des caméras de surveillance peuvent capter des images dans une rue d'un centre-ville sans que tous les passants y aient consenti, l'implantation d'une puce d'IRF sous-cutanée peut s'avérer presque impossible à refuser pour certaines catégories de personnes. Différentes dispositions légales encadrent le consentement à la collecte et à la communication des renseignements personnels recueillis par des NTSC. Cependant, certaines de ces dispositions comportent des limites. La Commission insiste donc sur la nécessité de mettre en place des moyens permettant aux citoyens de faire valoir leurs doléances, le cas échéant, et que celles-ci soient prises en considération.

En outre, la Commission estime que les citoyens devraient être mieux informés notamment et non exclusivement à l'égard des points suivants :

- les dispositions juridiques entourant le déploiement des NTSC, la collecte, l'utilisation, la communication et la conservation des renseignements personnels ;
- les risques, les inconvénients, les avantages et les bénéfices potentiels entraînés par le déploiement des NTSC ;
- les lieux et les documents soumis à la surveillance ;
- les moyens mis à la disposition des citoyens pour qu'ils participent au déploiement des NTSC, ce qui favoriserait un processus ouvert et transparent ;
- les moyens mis à la disposition des citoyens pour qu'ils fassent connaître leur opinion en la matière, voire leurs plaintes, que ce soit sur le déploiement des NTSC en général ou sur un projet de déploiement de NTSC en particulier.

Dans l'esprit du principe de représentativité, en vertu duquel ce sont des élus qui prennent les décisions politiques et non l'ensemble des citoyens, la Commission estime que, si le déploiement des NTSC se fait de manière transparente et en accord avec les valeurs fondamentales des sociétés démocratiques, chaque individu n'a pas nécessairement à donner son consentement. Il est cependant essentiel de réunir certaines conditions permettant d'éclairer le processus qui mène au déploiement des NTSC et de donner toute la marge de manœuvre nécessaire aux opposants et aux critiques afin que ceux-ci puissent exprimer leur point de vue.

En lien avec l'enjeu du consentement, la Commission tient à mettre en garde les citoyens quant au caractère invisible du déploiement des NTSC. L'objectif de plusieurs promoteurs des NTSC est d'ailleurs d'intégrer ces technologies dans l'environnement en les camouflant. Selon la Commission, cette façon de faire peut avoir des répercussions sur l'autonomie des citoyens et sur le respect de leur vie privée.

Le respect des finalités

Le respect des finalités explicitées pour lesquelles les NTSC sont déployées et l'exploitation de toutes les utilisations possibles de ces dernières sont source de tensions. D'une part, le respect des finalités explicitées est un principe important qui tend à prévenir les détournements d'usage et certaines formes d'abus et de dérives. D'autre part, l'exploitation de toutes les utilisations possibles des NTSC (y compris des fins auxquelles les personnes n'ont pas consenti) permettrait probablement d'accroître la sécurité.

Devant les exemples portés à son attention, la Commission s'inquiète des glissements qu'elle observe et de ceux qui risquent de se produire dans un avenir rapproché. Des normes, des procédés, des pratiques, des moyens de surveillance et de contrôle mis en place dans la foulée d'attentats terroristes sont progressivement intégrés à la lutte à la petite délinquance, puis ils sont récupérés par le secteur commercial. À l'inverse, des technologies comme l'IRF (identification par radiofréquence), dont les applications sont souvent associées au commerce de détail et à la gestion des inventaires, semblent vouloir coloniser le domaine de la sécurité. Aussi, considérant la facilité avec laquelle les NTSC trouvent des applications et donc les finalités qui peuvent être très différentes, il convient de rester vigilant à cet égard.

La durée de conservation des données collectées par les NTSC constitue un paramètre important dans les risques de détournement d'usage. Le principe est simple : moins longtemps les données sont conservées, moins les risques de détournement d'usage sont grands. Par conséquent, il est important de prévoir la durée de conservation des enregistrements avant la mise en place d'un système de surveillance, cette durée ne devant pas excéder la durée normale de conservation nécessaire dans le cadre de la fin visée.

Enfin, la Commission veut attirer l'attention sur le fait que l'analyse des renseignements personnels recueillis par les NTSC comporte des risques en matière de discrimination et de stigmatisation. Étant donné la nature des renseignements personnels recueillis et la possibilité d'en extraire des informations sur l'origine ethnique et sur la santé des usagers, sur les habitudes de consommation et leur affiliation avec des partis politiques, la question des risques de discrimination et de stigmatisation se pose avec acuité. Bien que les systèmes de surveillance ne soient pas mis en place dans le but de créer de la discrimination et de la stigmatisation, la Commission considère qu'il s'agit d'un détournement d'usage aussi vraisemblable qu'inacceptable.

Malgré tout, les NTSC offrent un potentiel très intéressant en matière de surveillance, ainsi que pour l'évaluation et la gestion des risques sur le plan de la sécurité. Ce point ne doit être ni négligé ni sous-estimé. Si d'aucuns voient dans la popularité croissante des moyens de surveillance une menace pour les droits et libertés des citoyens dans une société démocratique, les plus optimistes feront valoir que ces mêmes moyens peuvent contribuer à la prévention de la criminalité, voire du terrorisme.

Bien qu'ils puissent servir la prévention du crime, les détournements d'usage posent des risques de dérives et d'abus qui commandent une grande attention. En donnant l'aval à l'exploitation de toutes les utilisations possibles des NTSC afin de protéger la démocratie et l'ordre public contre le terrorisme et les autres formes de criminalité, la Commission craint justement le sacrifice de droits et de libertés qui fondent la démocratie. La Commission insiste tout au long du présent avis sur la nécessité de trouver des équilibres et elle en vient à la conclusion que la démocratie elle-même constitue un équilibre toujours fragile entre la liberté et la répression. Elle estime que les NTSC peuvent faire beaucoup pour améliorer la sécurité du public, mais croit par ailleurs qu'il n'est pas toujours nécessaire d'exploiter toutes les utilisations possibles qui leur sont associées pour assurer un niveau acceptable de sécurité.

La protection des renseignements personnels

La question des NTSC est souvent ramenée à un seul enjeu : la protection des renseignements personnels. Cette importance est notamment due au fait que les NTSC sont principalement déployées pour recueillir des renseignements (qui sont souvent personnels). Cet enjeu, plus que tout autre, concerne les valeurs de respect de la vie privée et de sécurité. Si, d'un côté, les renseignements personnels en disent long sur la vie privée des personnes, ils sont souvent vus comme une source riche d'informations permettant d'améliorer la sécurité.

La protection des renseignements personnels est presque systématiquement associée au respect de la vie privée. Il est vrai que les renseignements dits personnels ouvrent une fenêtre sur divers aspects de notre vie privée. En fait, la protection des renseignements personnels constitue un moyen d'actualiser la valeur de la vie privée. Si la première est davantage un concept juridique, le respect de la vie privée, dans le cadre du présent avis, doit être entendu comme une valeur.

Les données recueillies par des systèmes biométriques, par la vidéosurveillance et par l'IRF sont presque systématiquement des renseignements personnels. Par conséquent, le niveau de respect de la vie privée des personnes objets de la surveillance variera en fonction de l'utilisation, de la communication et de la conservation qui seront faites de ces données.

La protection des renseignements personnels est indissociable des systèmes biométriques, car les mesures biométriques sont considérées comme des renseignements personnels. Le fait que certaines données biométriques constituent des identifiants intimes bavards explique probablement pourquoi les systèmes biométriques font parfois craindre le pire en ce qui a trait au respect de la vie privée des personnes. Les données biométriques peuvent être qualifiées d'identifiants intimes, du fait qu'elles sont étroitement liées à l'individu auquel elles se rapportent. Le caractère bavard de certains identifiants biométriques constitue également un objet d'inquiétude :

les données biométriques portent en elles-mêmes plus d'informations que la simple reproduction de l'image d'une empreinte digitale, par exemple. En effet, selon certains experts, il est même possible de récolter des informations sur l'état de santé ou encore sur l'humeur des individus seulement par l'analyse des empreintes digitales ou encore de la rétine. Les personnes préfèrent généralement que certaines informations qui sont en leur possession et qui les concernent personnellement demeurent confidentielles ou, du moins, qu'elles soient traitées comme telles.

Par son caractère invisible et distant, la vidéosurveillance peut représenter une menace pour la vie privée. En effet, la technologie permet de filmer des personnes à leur insu, tant dans des lieux publics que dans des endroits privés. Or, en circulant dans des lieux publics, une personne doit admettre qu'elle ne bénéficie pas de la même intimité que dans sa maison, par exemple. Toutefois, ce serait abuser de ce principe que de prétendre que la personne renonce totalement au respect de sa vie privée dans les lieux publics. Toute personne est aussi en droit de circuler dans des lieux publics sans être constamment l'objet d'une surveillance. Le respect de la vie privée s'applique même dans des lieux publics.

Tout comme la vidéosurveillance, l'identification par radiofréquence (IRF) peut s'avérer une méthode subreptice de surveillance et être utilisée pour suivre des personnes à la trace. C'est pourquoi les commentaires de la Commission au sujet de la vidéosurveillance s'appliquent aussi dans le cas de l'IRF. Cependant, la Commission désire attirer l'attention sur le fait que la nature des renseignements personnels recueillis est différente. Dans le cas de la vidéosurveillance, ce sont les images captées et donc possiblement le visage des personnes qui seront les renseignements personnels. Pour l'IRF, des renseignements personnels cruciaux sont susceptibles d'être recueillis et utilisés : informations sur le crédit, la santé, l'identité, la nationalité, etc. La nature de ces renseignements pose donc des risques accrus d'atteinte à la vie privée des citoyens.

Considérant que les nouveaux passeports des citoyens de la plupart des membres de l'Union européenne et ceux maintenant délivrés aux citoyens américains comportent une puce d'IRF et devant l'intérêt déjà manifesté par le gouvernement du Canada pour l'introduction de données biométriques dans les documents d'identité des citoyens canadiens, la Commission estime qu'il faut rapidement statuer sur la manière d'encadrer l'introduction de ces technologies dans les documents d'identité. En outre, les expériences européenne et américaine montrent l'importance de protéger les renseignements personnels de manière adéquate si l'objectif de sécurisation des documents d'identité doit être atteint. Pour sa part, et considérant les risques élevés en matière de respect de la vie privée et de protection des renseignements personnels, la Commission estime important que le gouvernement du Québec travaille de concert avec les instances concernées au sein du gouvernement du Canada pour que, dans l'éventualité d'une introduction de puces d'IRF dans les documents d'identité des Canadiens, ces puces d'IRF contenant des renseignements personnels soient dotées d'un procédé de chiffrement qui permette de sécuriser les données et, ainsi, de mieux protéger la vie privée et d'assurer une meilleure protection des renseignements personnels.

Il serait inacceptable que des décisions basées sur des traitements automatisés deviennent monnaie courante dans le milieu de la surveillance et du contrôle de l'identité. La déshumanisation complète de la décision sécuritaire doit être évitée. Ici encore, il semble qu'un équilibre doit être atteint entre la part dévolue aux personnes et celle confiée à la machine en ce qui a trait à la surveillance et aux traitements des données recueillies. D'un côté, plus la part de gestion et d'administration des systèmes de surveillance est l'affaire de personnes, plus il faut s'attendre à ce que les expériences de vie de ces gestionnaires influent parfois sur leurs décisions. Mais il est inutile de se leurrer : personne n'est en mesure de faire totalement abstraction de ses opinions personnelles dans la conduite de son travail. D'autre part, si le traitement automatisé et informatisé des données peut réduire la part de l'influence des opinions et des préjugés des opérateurs de systèmes de surveillance, il n'en demeure pas moins inquiétant de savoir que des décisions préjudiciables peuvent être prises sur la base de ce traitement sans que qui que ce soit ait pu remettre en contexte les informations traitées.

Enfin, il faut se demander si le niveau de protection des renseignements personnels est le même d'un pays à l'autre et si le transfert de ces renseignements d'un pays doté de mesures favorisant largement la protection des données personnelles vers un pays qui n'a pas autant à offrir est acceptable. Déjà, les consommateurs traitent sur Internet

avec des entreprises de l'extérieur du pays qui conservent des renseignements personnels à leur égard, sans qu'ils connaissent toujours la manière dont ces renseignements seront protégés. Or, dans ces cas, les consommateurs sont toujours libres de ne pas effectuer ce genre de transactions. Mais en ce qui concerne des renseignements obtenus par le moyen de NTSC, les personnes ne savent pas toujours que des renseignements personnels les concernant seront conservés. Manifestement, une telle perspective n'est pas sans poser la question du contrôle de l'individu sur la direction que peuvent prendre ses renseignements personnels.

Le présent avis met en lumière des questions auxquelles la Commission n'est pas en mesure de répondre et dont elle ne peut assurer le suivi. Toutefois, celle-ci estime que plusieurs actions doivent être entreprises pour apporter des solutions et que les acteurs gouvernementaux en mesure de les accomplir sont facilement identifiables.

Considérant que le ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information a pour mandat de conseiller le gouvernement en lui fournissant des avis en matière d'accès à l'information et de protection des renseignements personnels, notamment lors de la présentation de projets de loi ou du développement de systèmes d'information et qu'à cette fin il peut consulter la Commission d'accès à l'information ;

Considérant que la Commission d'accès à l'information est chargée d'assurer le respect et la promotion de l'accès aux documents et de la protection des renseignements personnels et qu'elle peut prescrire des conditions applicables à un fichier de renseignements personnels auxquelles l'organisme public doit se conformer ;

Considérant que la Commission d'accès à l'information peut également, au terme d'une enquête relative à la collecte, à la détention, à la communication ou à l'utilisation de renseignements personnels par une personne qui exploite une entreprise, après lui avoir fourni l'occasion de présenter ses observations, lui recommander ou lui ordonner l'application de toute mesure corrective propre à assurer la protection des renseignements personnels ;

Et considérant que la Commission des droits de la personne et des droits de la jeunesse du Québec a notamment pour mandats :

- *d'élaborer et d'appliquer un programme d'information et d'éducation, tant en matière de droits de la personne que de protection des droits de la jeunesse ;*
- *de diriger et encourager les recherches et les publications sur les libertés et droits fondamentaux et sur les droits de la jeunesse ;*
- *de recevoir les suggestions, recommandations et demandes touchant les droits et libertés de la personne, en tenant des auditions publiques au besoin, et d'adresser au gouvernement les recommandations appropriées ;*
- *de coopérer avec toute organisation vouée à la promotion des droits et libertés de la personne, au Québec ou à l'extérieur,*

la Commission recommande au ministre responsable des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'Accès à l'information, à la Commission d'accès à l'information et à la Commission des droits de la personne et des droits de la jeunesse du Québec de collaborer ensemble dans le but de mettre en œuvre les actions suivantes :

1. **Favoriser le dialogue entre les citoyens, le gouvernement et l'industrie en vue d'adopter des lignes directrices pour l'utilisation de ces technologies qui tiennent compte des préoccupations éthiques en la matière et des valeurs fondamentales des sociétés démocratiques.**
2. **Suivant une approche consultative, conseiller le gouvernement dans ses projets de déploiement de NTSC, notamment sur les aspects soulevant des enjeux éthiques et à la lumière des critères de pertinence, d'efficacité et de fiabilité.**
3. **Organiser une consultation de la population (sur le modèle du forum citoyen tel qu'élaboré par le Commissaire à la santé et au bien-être) qui ferait une place importante aux enjeux éthiques.**
4. **Diffuser les résultats de cette consultation dans la population afin de la sensibiliser aux questions d'éthique associées aux NTSC.**
5. **Informer la population quant aux dispositions juridiques entourant le déploiement des NTSC, à ses conséquences pour les valeurs d'autonomie, de liberté, de sécurité et de vie privée et aux moyens mis à la disposition des citoyens pour participer à la prise de décision, à la mise en œuvre et au suivi en la matière.**
6. **Mettre en place un mécanisme de réparation et de rectification pour les cas où l'utilisation des NTSC cause des préjudices à des personnes en les associant à tort à des activités illicites.**

Liste des membres de la Commission[237]

Présidente

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

Membres

Frédéric Abraham
Doctorant en philosophie
Université du Québec à Trois-Rivières

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

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

Hubert Doucet
Programmes de bioéthique
Université de Montréal

Benoît Gagnon
Chercheur
Centre international de criminologie comparée (CICC)
Université de Montréal

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

Patrice K. Lacasse
Coordonnateur du Bureau de développement social
des Premières Nations du Québec
Commission de la santé et des services sociaux
des Premières Nations du Québec et du Labrador

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

Dany Rondeau
Professeure
Département des sciences humaines
Université du Québec à Rimouski

Andy Sheldon
Président et chef de la direction
Medicago inc.

Eliana Sotomayor
École de service social
Université de Montréal

Membre invitée

M^e Danielle Parent
Directrice des affaires juridiques
Commissaire au lobbyisme du Québec

Coordonnatrice

M^e Nicole Beaudry, notaire

237. Au moment de l'adoption de l'avis.