RAPPORT PRÉLIMINAIRE #2 DU LOT 5 DU PROJET ÉLABORATION DES STANDARDS POUR L'IDO

APPORTS POUR UN CADRE CONCEPTUEL POUR LA GESTION DES ENJEUX SOCIAUX ET ÉTHIQUES DE L'IDO DANS LA VILLE

FÉVRIER 2018

Prepared for:

Ville de Montréal

À l'attention de M. Jean-Martin Thibault

Directeur (CTO) Architecture, innovation et sécurité – TI

Ville de Montréal

275 rue Notre-Dame Est

Montréal, QC, HCY 1C6

Canada

POLYTECHNIQUE MONTRÉAL

Ce rapport a été préparé par le Centre international de référence sur le cycle de vie des produits procédés et services (CIRAIG).

Fondé en 2001, le CIRAIG a été mis sur pied afin d'offrir aux entreprises et aux gouvernements une expertise universitaire de pointe sur les outils du développement durable. Le CIRAIG est un des plus importants centres d'expertise en cycle de vie sur le plan international. Il collabore avec de nombreux centres de recherche à travers le monde et participe activement à l'Initiative sur le cycle de vie du Programme des Nations Unies sur l'Environnement (PNUE) et de la Société de Toxicologie et de Chimie de l'Environnement (SETAC).

Le CIRAIG a développé une expertise reconnue en matière d'outils du cycle de vie incluant l'analyse environnementale du cycle de vie (ACV) et l'analyse sociale du cycle de vie (ASCV). Complétant cette expertise, ses travaux de recherche portent également sur l'analyse des coûts du cycle de vie (ACCV) et d'autres outils incluant les empreintes carbone et eau. Ses activités comprennent des projets de recherche appliquée touchant plusieurs secteurs d'activités clés dont l'énergie, l'aéronautique, l'agroalimentaire, la gestion des matières résiduelles, les pâtes et papiers, les mines et métaux, les produits chimiques, les télécommunications, le secteur financier, la gestion des infrastructures urbaines, le transport ainsi que de la conception de produits « verts ».

CIRAIG

Centre international de référence sur le cycle
de vie des produits, procédés et services
Polytechnique Montréal
Département de génie chimique
3333 Chemin Queen-Mary, suite 310
Montréal (Québec) Canada
H3V 1A2

www.ciraig.org

Équipe de travail

Équipe de recherche

Réalisation

Sara Russo Garrido

Supervision, recherche et rédaction

Marie-Luc Arpin

Révision

Direction de projet

Pr Nicolas Merveille Ph.D.

Professeur régulier, ESG UQAM et CIRAIG

Participants au projet pour la Ville de Montréal :

Jean-Martin Thibault, Pierre-Antoine Ferron, Stéphane Guidoin, Michel Charest, Song Nhi Nguyen, Martin-Guy Richard et Patrick Lozeau.

Sommaire

Rappel du mandat

Le présent rapport vise à lancer des pistes pour la définition d'un cadre conceptuel dont la Ville de Montréal pourrait s'inspirer pour implanter un programme d'analyse et de gestion des enjeux éthiques et d'acceptabilité sociale occasionnés par le système technologique et analytique de l'Internet des objets dans la ville. Ce système comprend la collecte de données d'origines multiples (p. ex : des capteurs installés par la ville, des réseaux sociaux, de bases de données externes), leur traitement, stockage et analyse interne, ainsi que leur ouverture, sous forme de bases de données, de visualisations, ou d'applications pour les citoyens. Le rapport s'inscrit dans la foulée de la revue de littérature sur les enjeux éthiques et l'acceptabilité sociale de l'Internet des objets[1] (Russo Garrido et al, 2017).

Dans le cadre du rapport, deux cadres sont présentés pour contribuer à la réflexion au sein de la Ville de Montréal pour le développement d'un (des) cadre(s) conceptuel(s) pour la gouverne éthique du système de l'IdO:

- des cadres visant à appuyer l'identification et l'analyse des enjeux éthiques et d'acceptabilité sociale au sein du système de l'IdO; et
- une liste de principes, visant à informer la gestion de ces enjeux.

Ces éléments ne constituent pas, à eux seuls, un cadre conceptuel complet. Cependant, ils sont des jalons non négligeables vers le développement d'un cadre plus complet et évolutif.

Cadres d'appui à l'identification des enjeux éthiques et sociaux

Les cadres d'appui à l'identification des enjeux éthiques et sociaux présentés dans ce rapport visent à fournir aux décideurs des outils qui puissent les assister dans leur identification et analyse des enjeux associés au projet de l'IdO. Ils reposent sur les sources d'information suivantes, la plupart issues de la revue de littérature (Russo Garrido et al, 2017) :

- les grandes composantes du système de l'IdO, tel qu'exploité par la Ville de Montréal; et
- les enjeux éthiques identifiés dans la revue de littérature et dans l'avis de la Commission d'éthique en sciences et technologie du Québec sur les villes intelligentes (CÉSTQ, 2017).

Les grandes composantes du système de l'IdO sont présentées dans la Figure ci-dessous.

[1] Le titre complet est : RAPPORT FINAL #1 POUR LE LOT 5 DU PROJET ÉLABORATION DES STANDARDS POUR L'IDO -- REVUE DE LITTÉRATURE : ENJEUX ÉTHIQUES ET ACCEPTABILITÉ SOCIALE DE L'IDO DANS LA VILLE INTELLIGENTE

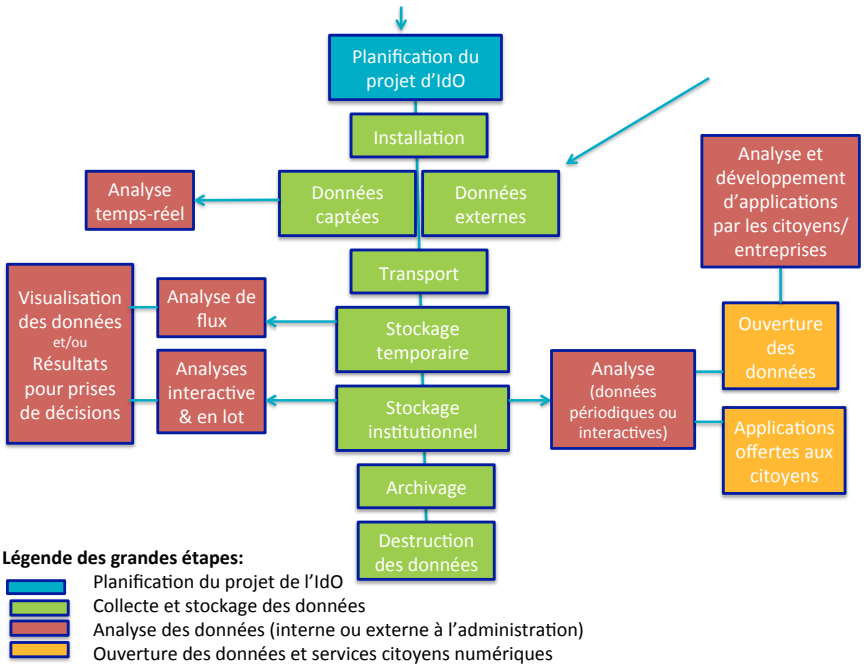


Figure A. Composantes du système de l'IdO de la Ville de Montréal.

Tel qu'expliqué dans la revue de littérature, les composantes peuvent être regroupées en 4 grandes étapes présidant à l'opération du système :

- La planification du projet de l'IdO;
- La collecte et le stockage des données;
- L'analyse des données (interne ou externe à l'administration municipale); et
- L'ouverture des données et services citoyens numériques.

Sur la base de ces composantes et des enjeux éthiques et sociaux identifiés dans la revue de littérature et l'avis de la CÉSTQ (2017), le cadre suivant est proposé en ce qui concerne l'identification à haut niveau des enjeux éthiques.

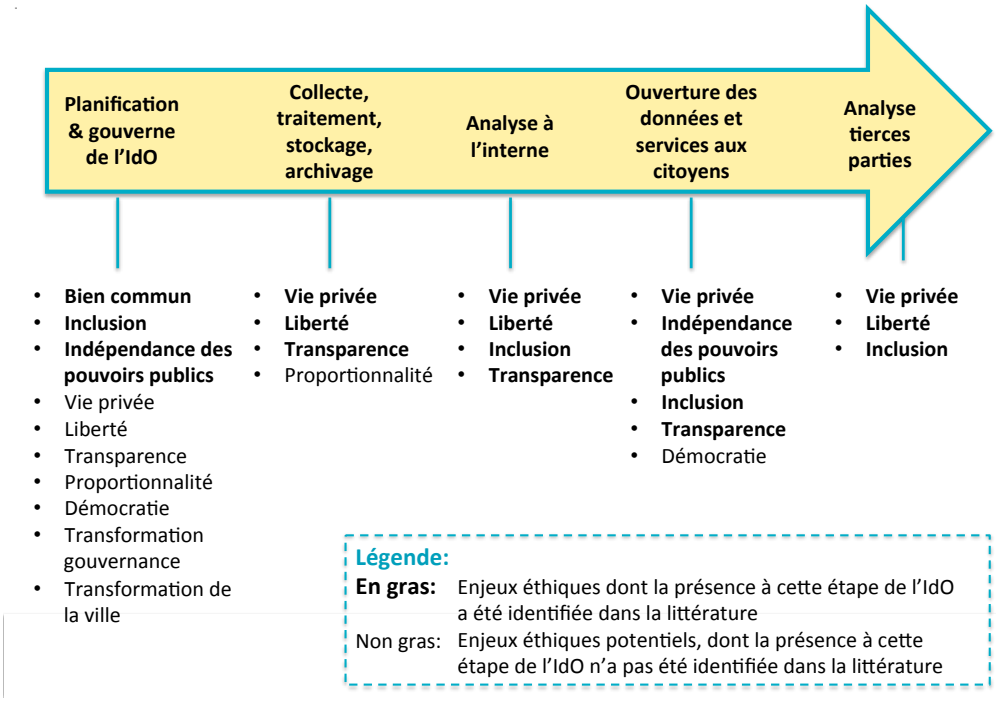


Figure B. Cadre général d'appui à l'identification à haut niveau des enjeux éthiques et d'acceptabilité sociale.

Bien qu'un cadre comme celui présenté ci-dessous puisse être utile pour des réflexions d'ordre général, il est également utile de faire usage de cadres beaucoup plus spécifiques, qui identifient non seulement les enjeux d'ordre général, mais décortiquent de façon plus détaillée les actions et situations qui peuvent donner lieu à l'émergence d'enjeux d'ordre éthique ou social. Les Figures C, D et E offrent ce niveau de détail, chacune pour un regroupement d'enjeux traités dans la revue de littérature, tel qu'identifié dans le nom des Figures.

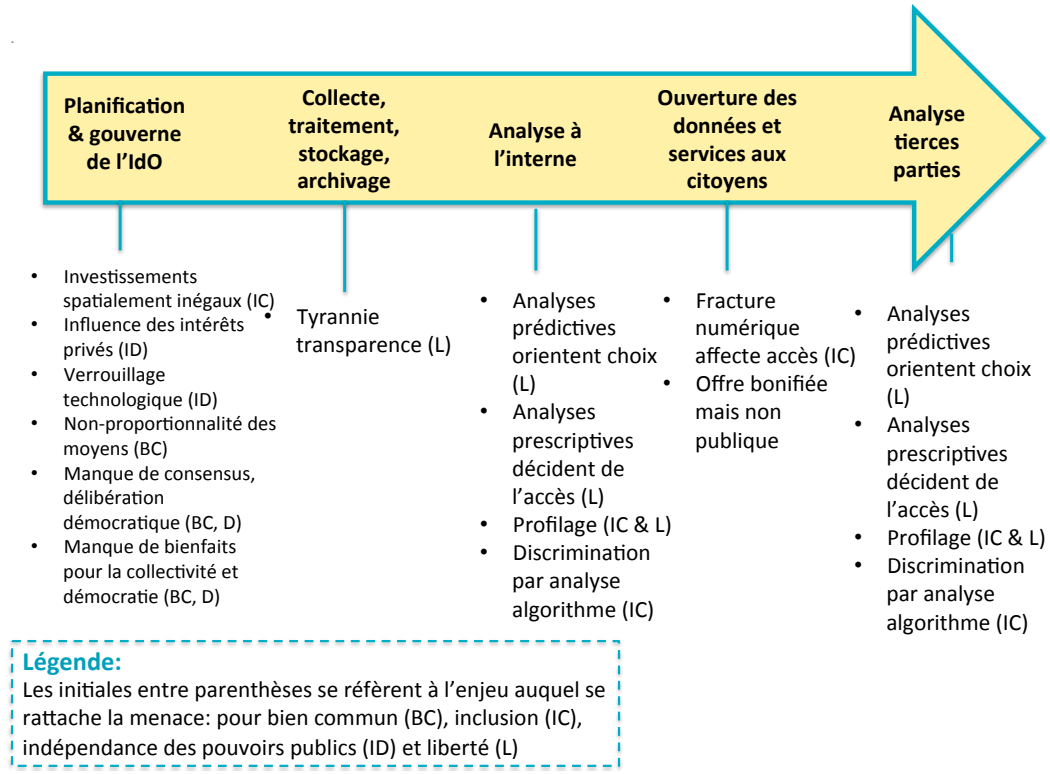


Figure C. Menaces associées aux enjeux du bien commun, l'inclusion, l'indépendance des pouvoirs publics et la liberté.

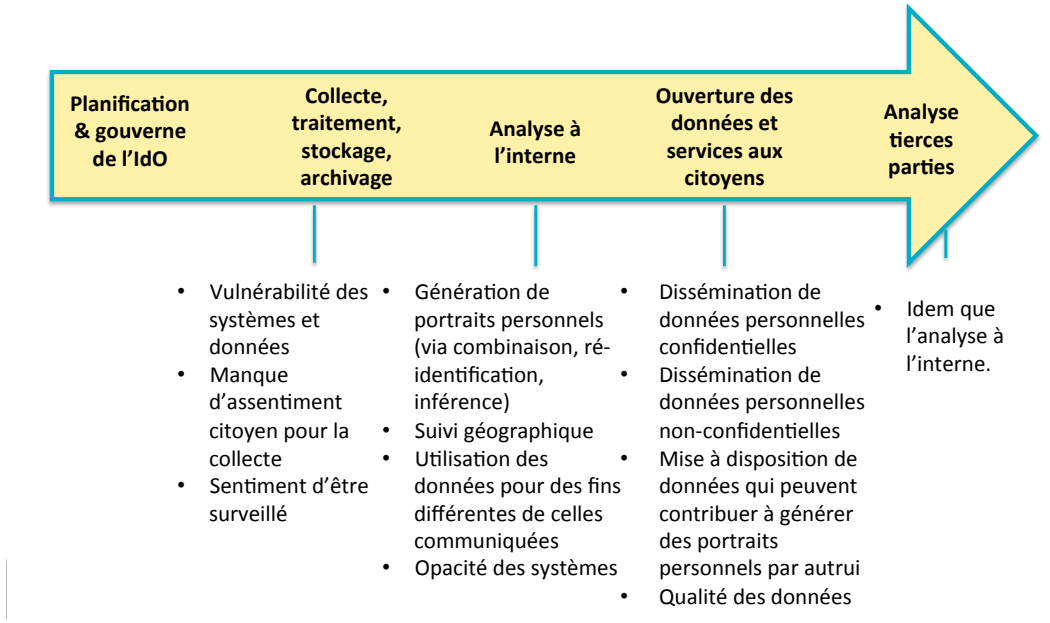


Figure D. Menaces associées aux enjeux de la vie privée et de la transparence.

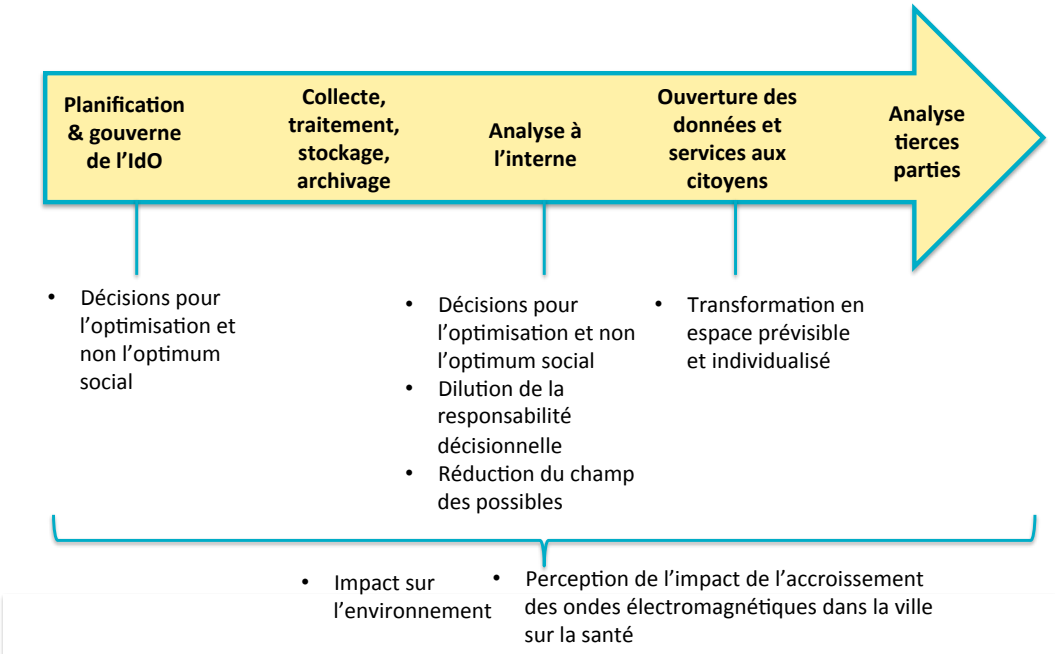


Figure E. Menaces associées à la transformation de la gouvernance et de la ville.

Liste de principes pour aborder l'analyse et la gestion des enjeux

Le développement d'une liste de principes pour aborder l'analyse et la gestion des enjeux est la seconde contribution de ce rapport. Cette liste vise à réunir en son sein les grands principes les plus pertinents afin de faire face aux enjeux éthiques et d'acceptabilité sociale occasionnés par le système de l'IdO. Elle vise à être une boussole qui permette d'aider à identifier la route à suivre dans un environnement caractérisé par le changement, l'innovation, la transformation du lien social et la perte de repères en matière éthique.

Afin de développer cette liste, il a été décidé de ne pas partir de zéro, mais bien de capitaliser sur toutes les réflexions existantes pertinentes. Ceci nous a poussé à réfléchir aux principes émis par rapport à l'Ido, la ville intelligente, l'intelligence artificielle et la recherche se basant sur des données massives. L'encadré ci-dessous décrit succinctement la démarche ayant été mise de l'avant.

Démarche employée pour développer la liste de principes

1. Réalisation de l'inventaire des listes de principes existantes pertinentes.
2. Extraction et analyse de tous les principes, de façon à voir les chevauchements et particularités.
3. Développement d'une liste finale de principes axée sur la pertinence par rapport à l'IdO et la complétude par rapport aux listes consultées.
4. Analyse des chevauchements entre la liste proposée et les conclusions de la revue de littérature.
5. Identification des principes qui doivent être renforcés et des prochaines étapes

Les listes de principes existantes répertoriées ont été sélectionnées sur la base de deux critères : la pertinence et l'importance. Le tableau ci-dessous identifie les documents sélectionnés, classés selon les

composantes techniques ou thématiques auxquels ils se rapportent. Les listes de principes sont présentées plus en détail dans la Section 3.3.

Tableau A. Listes de principes considérées

Catégorie	Listes de principes
Principes normatifs relatifs à la vie privée	• Principes normatifs protection vie privée au Canada • *Fair Information Practice Principles (FIPPs)* • Lignes directrices de l'OCDE • Vie privée dès la conception • Sept principes de la protection intégrée de la vie privée de l'Ontario • Principes de la vie privée de la ville de Seattle • Législation européenne 1990 et 2018 (général)
Principes normatifs relatifs à l'IdO et la ville intelligente	• Recommandations de l'Avis de la Commission en éthique sciences et technologie du Québec sur la ville intelligente • Lignes directrices pour les villes intelligentes et équitables / *NYC IoT Guidelines*
Principes relatifs à l'intelligence artificielle[2]	• Principes de l'ASILOMAR pour l'IA bénéfique • *Fair Automation Practice Principles (FAPPs)* • Déclaration de Montréal pour un développement responsable de l'intelligence artificielle
Principes relatifs aux données massives[3]	• Dix règles pour la recherche responsable en données massives
Codes de conduite	• Code d'éthique et de conduite professionnelle de l'ACM • Code d'éthique de l'IEEE[4]

Sur la base des 13 documents présentés au Tableau A, une liste finale de principes a été développée. Ces principes ont ensuite été classifiés, résumés et distillés afin d'en arriver à une liste finale, avec les critères suivants en tête :

- Complétude : couvrir un maximum de thèmes identifiés dans les listes de principes consultés ;
- Pertinence : tous les thèmes directement pertinents à la gestion des enjeux éthiques et les différentes composantes techniques du système de l'IdO[5] ;

[2] Afin d'alimenter ultérieurement l'inventaire, la réflexion de l'IEE au sujet de l'intelligence artificielle pourrait être ajoutée à cette liste (IEEE, 2017).

[3] Afin d'alimenter ultérieurement l'inventaire, les principes présentés dans l'article de Richards et King (2014) pourraient être ajoutés ici.

[4] Il est à noter que l'ACM et l'IEEE ont produit un code ensemble, mais celui-ci n'a pas été considéré dans l'exercice. Étant donné que l'IEEE est entrain de réviser une nouvelle version de son code individuel, il a été perçu comme plus important de se coller aux codes les plus récents, plutôt qu'à ceux réalisés en collaboration.

- Du général au spécifique : Identifier un nombre restreint de principes généraux et décliner, sous ceux-ci, des principes plus spécifiques.

Il est bien sûr à noter que le cadre proposé constitue une proposition de base. Il devra être appelé à évoluer et à se renforcer via la consultation/vérification d'autres documents de référence, via des délibérations au sein de la ville de Montréal, ainsi que des consultations plus élargies avec des parties prenantes.

Le tableau ci-dessous présente les 11 grands principes proposés. Ceux-ci peuvent ensuite être déclinés en sous-principes, ou principes spécifiques, tel que présenté dans l'Annexe G[6]. Il appartiendra à l'équipe de la Ville de décider les principes finaux retenus et leur niveau de spécificité souhaité.

Tableau B: Liste de principes proposée

Thème	Principe
Bien commun	Assurer que l'IdO soit au service du bien commun et de la recherche d'un optimum social.
Démocratie et participation citoyenne	Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique
Vie privée	Protéger et respecter la vie privée* des citoyens
Transparence	Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation
Sécurité	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Bonne gestion des données	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Évaluations et conséquences	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeurs sociales élargies
Équité et inclusion	Mettre tous les moyens en œuvre pour que le traitement accordé tous soit juste et impartial. Éviter le profilage, la discrimination et le renforcement des inégalités pour développer un projet inclusif
Autonomie des pouvoirs publics	Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés
Systèmes explicables	Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision, ainsi qu'une explication des données utilisées (quelle donnée, quelle source, comment est-elle mobilisée)
Liberté	Assurer que le citoyen puisse préserver son sentiment de liberté

[5] Cependant, les principes traitant de la bonne gouvernance générale de l'IdO (en termes de maintien d'infrastructure, d'opérationnalité, etc.), ont été évacués de l'exercice.

[6] Il est à noter que l'Annexe G présente également de manière transparente, l'origine de la formulation des grands principes proposés (de quelle liste, cadre ou code ils proviennent) ainsi que les listes de principes consultées qui coïncident sur différents sujets.

* Le concept de la vie privée fait l'objet de nombreux débats quant à sa définition. Ici, le terme est entendu comme la liberté des individus vis-à-vis toute intrusion physique, toute interférence dans leur vie personnelle et des entraves à leur capacité de contrôle de l'accès et de l'utilisation de leurs informations personnelles.

De façon générale, les enjeux et menaces documentés dans la revue de littérature (tel que présenté dans les Figures C, D et E) sont relativement bien couverts par le cadre de principes proposé. Seuls les enjeux de 'liberté' et de 'transformation de la ville' ne sont que partiellement couverts dans le cadre – quelques ajouts de principes (généraux ou spécifiques – à définir) ont été réalisés afin d'assurer une couverture complète, tel qu'expliqué dans la Section 4.1.

Prochaines étapes

Bien que la liste de principes proposée soit le résultat d'un travail méticuleux visant à rassembler les meilleurs principes existants à ce jour pour aborder les enjeux éthiques et sociaux du système de l'IdO, tel que planifié pour la ville de Montréal, plusieurs étapes doivent encore être franchies afin de parfaire cette liste et surtout, pour la rendre pleinement utile. La Section 4.2 présente des étapes ultérieures recommandées pour une amélioration future de la liste, y compris : 1) Débattre, reformuler au besoin, sélectionner et valider des 10 principes proposés et leurs principes spécifiques afférents – à l'intérieur de l'administration municipale et à l'extérieur de celle-ci ; 2) identifier les principes spécifiques manquants ; 3) renforcer les principes spécifiques faibles – tel que discuté dans la Section 4.1 ; et 4) identifier comment le cadre se décline en pratiques spécifiques à différentes étapes du système de l'IdO. En effet, il est impératif de pouvoir traduire les principes énoncés en pratiques spécifiques, applicables dans le quotidien des fonctionnaires de l'administration publique.

Conclusion

En somme, les cadres proposés dans ce rapport visent à alimenter la réflexion au sein de la Ville de Montréal sur le développement d'un (des) cadre(s) conceptuel(s) pour la gouverne éthique du système de l'IdO. Tel que mentionné précédemment, ces éléments ne constituent pas, à eux seuls, des cadres conceptuels complets. Cependant, ils sont des jalons non négligeables vers le développement d'un cadre évolutif plus complet. À terme, ces éléments pourront porter main forte à l'implantation de pratiques optimales d'analyse, de gestion et d'intervention en matière d'enjeux éthiques et d'acceptabilité sociale en lien avec le système de l'IdO au sein de la Ville de Montréal. En effet, on ne peut faire face à l'incertitude et les transformations occasionnées par l'implantation de nouvelles technologies dans la Ville qu'en se dotant d'outils pour appuyer la veille continuelle des enjeux émergeants et le développement de principes et pratiques afférentes pour contribuer à débattre des marches à suivre et des choix de société à opérer.

Table des matières

Liste des tableaux

Liste des figures

Abbreviations and acronyms

ACM	Association of Computing and Machinery
CÉSTQ	Commission d'éthique en sciences et technologies du Québec
FAPPs	*Fair Automation Practice Principles*
FIPPs	*Fair Information Practice Principles*
IA	Intelligence artificielle
IdO	Internet des objets
IEEE	*Institute of Electrical and Electronics Engineers*
NYC	New York City
OCDE	Organisation de coopération et de développement économique

1 Introduction

Le présent rapport vise à lancer des pistes pour la définition d'un cadre conceptuel dont la Ville de Montréal pourrait s'inspirer pour implanter un programme d'analyse et de gestion des enjeux éthiques et d'acceptabilité sociale occasionnés par le système technologique et analytique de l'Internet des objets dans la ville. Ce système comprend la collecte de données d'origines multiples (p. ex : des capteurs installés par la ville, des réseaux sociaux, de bases de données externes), leur traitement, stockage et analyse interne, ainsi que leur ouverture, sous forme de bases de données, de visualisations, ou d'applications pour les citoyens. Le rapport s'inscrit dans la foulée de la revue de littérature sur les enjeux éthiques et l'acceptabilité sociale de l'Internet des objets[7] (Russo Garrido et al, 2017).

Le rapport s'inscrit dans la foulée de la revue de littérature sur les enjeux éthiques et l'acceptabilité sociale de l'Internet des objets (Russo Garrido et al, 2017), qui a identifié les enjeux les plus probables pour la ville, sur la base d'analyses multiples et d'expériences passées de municipalités à travers le monde. Son objectif est de contribuer à la réflexion au sein de la Ville de Montréal pour le développement d'un (des) cadre(s) conceptuel(s) pour la gouverne éthique du système de l'IdO. Pour ce faire, deux cadres sont proposés pour alimenter le processus :

- un cadre visant à appuyer l'identification et l'analyse des enjeux éthiques et d'acceptabilité sociale au sein du système de l'IdO; et
- une liste de principes, visant à informer la gestion de ces enjeux.

Ces éléments ne constituent pas, à eux seuls, un cadre conceptuel complet. Cependant, ils sont des jalons non négligeables vers le développement d'un cadre plus complet et évolutif.

La Section 2 de ce rapport s'attardera d'abord au premier cadre d'identification des enjeux. Ce dernier découle en grande partie des résultats de la revue de littérature susmentionnée. La Section 3 s'attardera quant à lui à expliquer la démarche employée pour développer une liste de principes. La Section 4 présentera la liste de principes. Finalement, la conclusion résumera la démarche développée jusqu'ici ainsi que les prochaines étapes logiques à enclencher.

[7] Le titre complet est : RAPPORT FINAL #1 POUR LE LOT 5 DU PROJET ÉLABORATION DES STANDARDS POUR L'IDO -- REVUE DE LITTÉRATURE : ENJEUX ÉTHIQUES ET ACCEPTABILITÉ SOCIALE DE L'IDO DANS LA VILLE INTELLIGENTE

2 Cadre d'appui à l'identification des enjeux

Le cadre d'appui à l'identification des enjeux éthiques et sociaux vise à fournir aux décideurs un cadre qui puisse les assister dans leur identification et analyse des enjeux associés au projet de l'IdO. Ce cadre repose sur deux grands axes :

- les grandes composantes du système de l'IdO, tel qu'exploité par la Ville de Montréal; et
- les enjeux éthiques identifiés dans la revue de littérature (Russo Garrido et al, 2017) et dans l'avis de la Commission d'éthique en sciences et technologie du Québec (CÉSTQ, 2017).

En bref, ce cadre met à plat les conclusions de la revue de littérature qui a constitué la première partie du mandat actuel et y ajoute quelques nouveautés issues de l'avis de la CÉSTQ (2017). Il ne comporte donc pas de recherche originale, mais présente un nouvel agencement des informations présentées dans le 1er rapport du mandat.

2.1 Grandes composantes du système de l'IdO

Tel que mentionné en introduction, le système de l'IdO comprend la collecte de données d'origines multiples (p. ex : des capteurs installés par la ville, des réseaux sociaux, de bases de données externes), leur traitement, leur stockage et leur analyse, ainsi que leur ouverture, sous forme de bases de données, de visualisations, ou d'applications pour les citoyens. De façon simplifiée, le système de l'IdO de la Ville de Montréal se décompose tel que présenté dans la Figure ci-dessous.

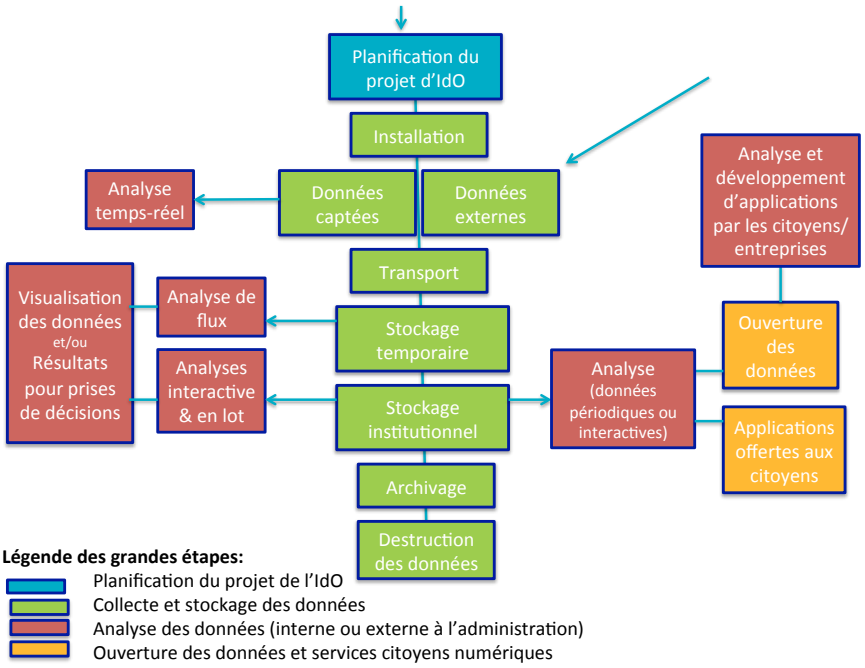


Figure 1. Composantes du système de l'IdO de la Ville de Montréal.

Tel qu'expliqué dans le rapport de revue de littérature, les composantes peuvent être regroupées en 4 grandes étapes présidant à l'opération du système :

- La planification du projet de l'IdO;
- La collecte et le stockage des données;
- L'analyse des données (interne ou externe à l'administration municipale); et
- L'ouverture des données et services citoyens numériques.

2.2 Enjeux identifiés dans la revue de littérature

Les enjeux éthiques et les enjeux potentiels en matière d'acceptabilité sociale identifiés dans la revue de littérature sont résumés dans les Figures 2, 3, et 4. Ceux-ci sont listés en fonction de la grande étape du système IdO dans lequel ils interviennent. Les menaces spécifiques à ces étapes qui donnent lieu à ces enjeux éthiques potentiels sont également spécifiés, tel que repéré dans la littérature.

La Figure 4 fait également état des enjeux éthiques pertinents à l'IdO identifiés dans l'avis sur la ville intelligente de la Commission d'éthique en sciences et technologies du Québec (CÉSTQ, 2017). Il ne s'agit pas de l'intégralité des éléments identifiés par la CÉSTQ, mais bien une liste *pertinente* à l'IdO et *complémentaire* aux enjeux répertoriés dans la revue de littérature.

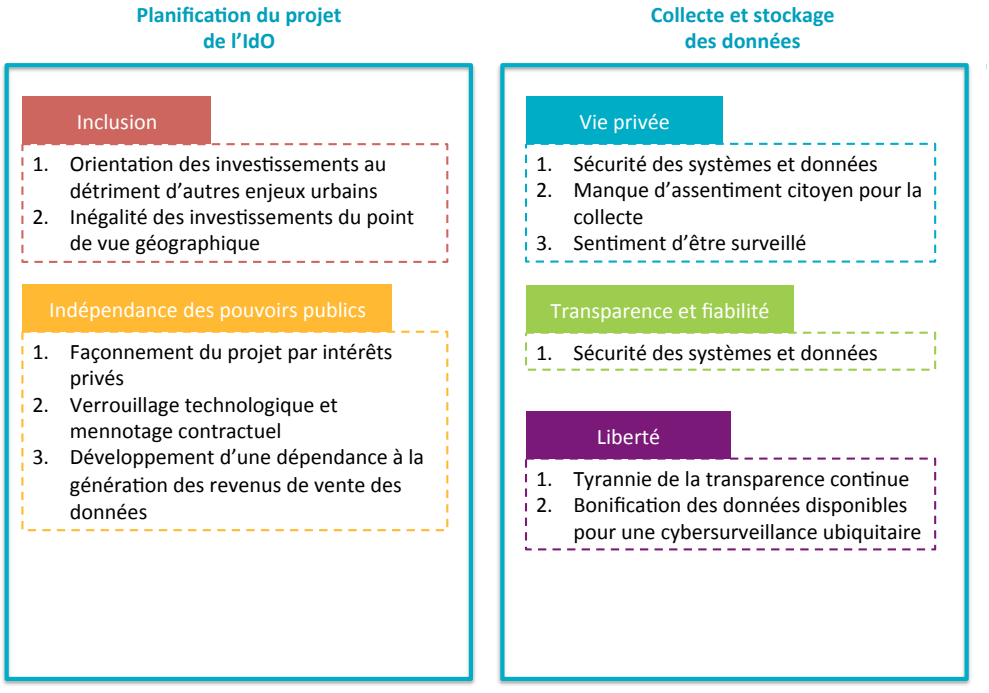


Figure 2. Enjeux éthiques et menaces associées à l'étape de la planification et de la collecte et stockage des données.

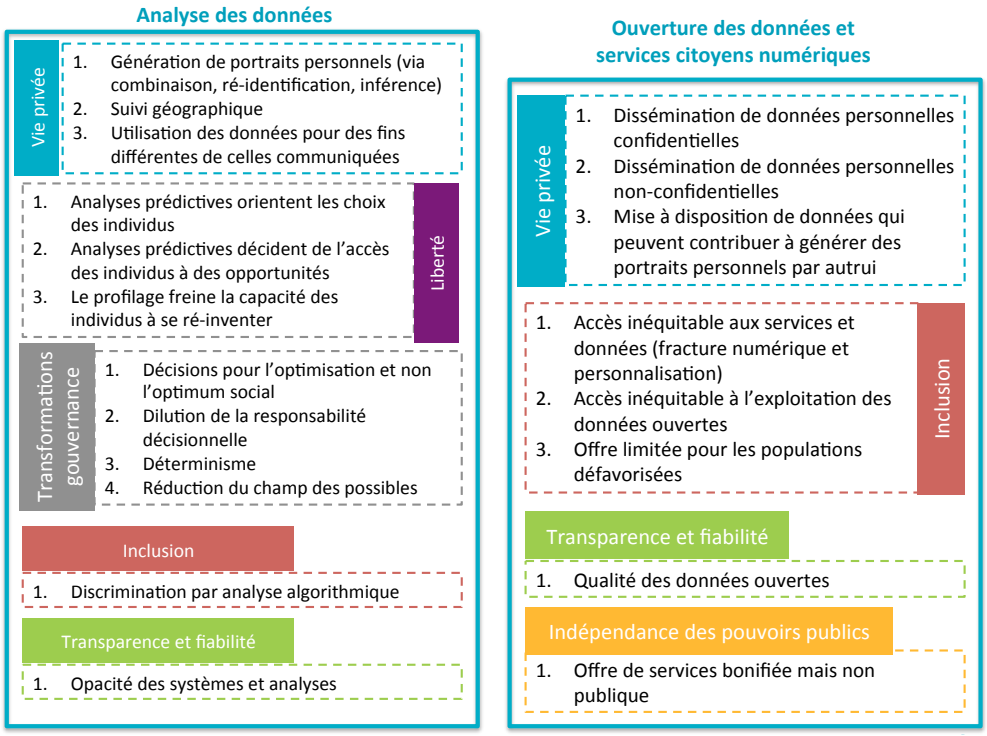


Figure 3: Enjeux éthiques et menaces associées à l'étape de l'analyse et l'ouverture des données.

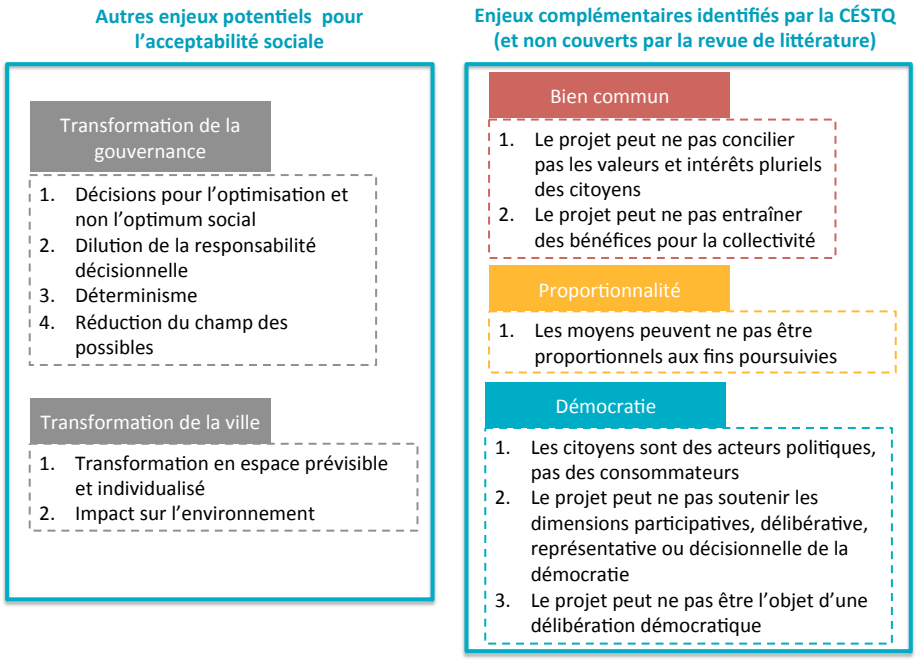


Figure 4: Autres enjeux en lien avec l'acceptabilité sociale et de l'avis de la CÉSTQ.

2.3 Cadres proposés pour l'appui à l'identification d'enjeux

Sur la base des grandes composantes du système de l'IdO et les enjeux éthiques et sociaux identifiés dans la revue de littérature et l'avis de la Commission d'éthique en sciences et technologie du Québec, le cadre suivant est proposé en ce qui concerne l'identification à haut niveau des enjeux éthiques. Tel que mentionné dans la légende, les enjeux inscrits en caractère gras correspondent aux enjeux éthiques dont la présence à cette étape de l'IdO (e.g., la planification, l'analyse, etc.) a été identifiée dans la littérature. Les enjeux écrits en caractère non gras correspondent à des enjeux potentiels, dont la présence à cette étape n'a pas été identifiée dans la littérature, mais qui pourraient potentiellement tout de même être présents.

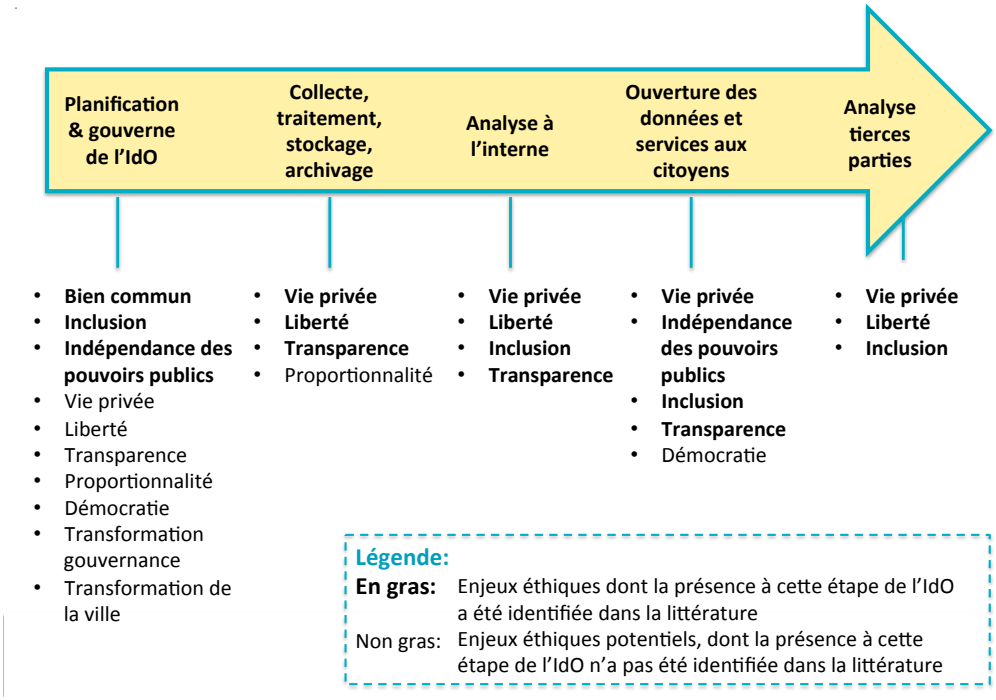


Figure 5. Cadre général d'appui à l'identification des enjeux éthiques et d'acceptabilité sociale.

Bien qu'un cadre comme celui présenté ci-dessous puisse être utile pour des réflexions d'ordre général, il est également utile de faire usage de cadres beaucoup plus spécifiques, qui identifient non seulement les enjeux d'ordre général, mais décortiquent de façon plus détaillée les actions et situations qui peuvent donner lieu à l'émergence d'enjeux d'ordre éthique ou social. Les Figures suivantes offrent ce niveau de détail. La Figure 6 se concentre sur les enjeux et les menaces associées avec la vie privée et la transparence; la Figure 7 se concentre sur les enjeux et les menaces associées avec le bien commun, l'inclusion, l'indépendance des pouvoirs et la liberté; et la Figure 8 se penche sur les enjeux et les menaces associées avec la transformation de la gouvernance et de la ville.

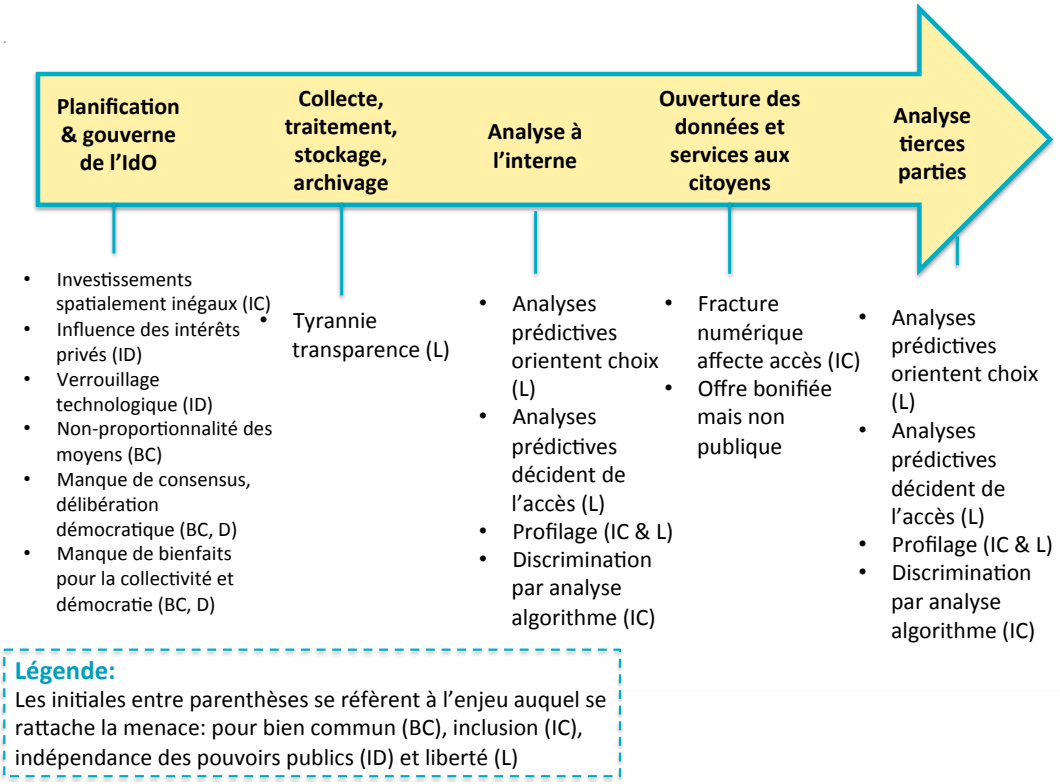


Figure 6. Menaces associées aux enjeux du bien commun, l'inclusion, l'indépendance des pouvoirs publics et la liberté.

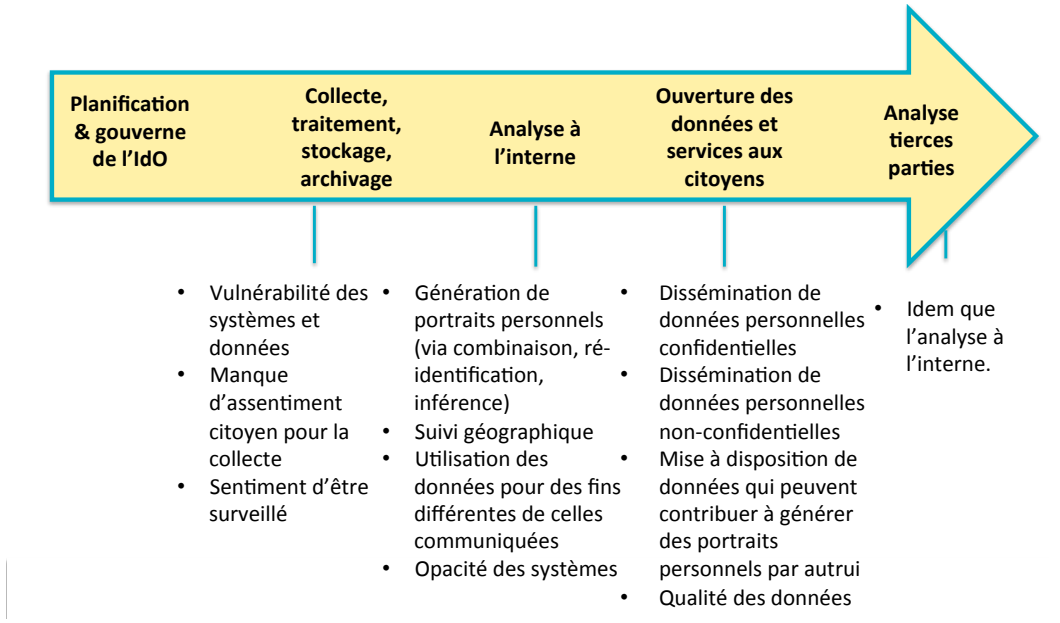


Figure 7. Menaces associées aux enjeux de la vie privée et de la transparence.

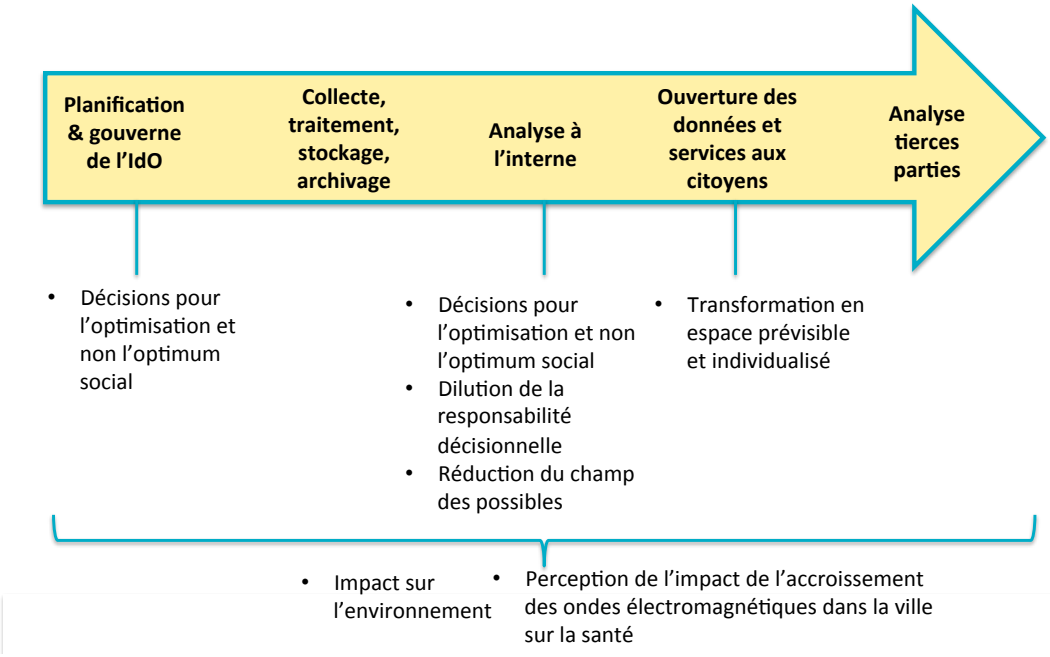


Figure 8. Menaces associées à la transformation de la gouvernance et de la ville.

3 Liste de principes pour aborder l'analyse et la gestion d'enjeux

La liste de principes pour aborder l'analyse et la gestion des enjeux vise à réunir en son sein les grands principes les plus pertinents afin de faire face aux enjeux éthiques et d'acceptabilité sociale occasionnés par le projet de l'IdO. La liste vise à définir une orientation et des règles de base pour pouvoir analyser et traiter les cas les plus épineux qui émergeront dans le cadre de ce projet. En ce sens, la liste de principes vise à être une boussole qui permette d'énoncer la route à suivre dans un environnement caractérisé par le changement, l'innovation, la transformation du lien social et la perte de repères en matière éthique.

3.1 Démarche

Afin de développer une liste de principes pour aborder l'analyse et la gestion des enjeux éthiques de l'IdO dans la ville, il a été décidé de ne pas partir de zéro, mais bien de capitaliser sur toutes les réflexions existantes sur chacune des composantes technologiques et analytiques qui composent le système de l'IdO. Ceci nous a poussé à réfléchir aux principes émis par rapport à l'Ido, la ville intelligente, l'intelligence artificielle et la recherche se basant sur des données massives. Cette matière a été analysée, de façon à identifier les chevauchements entre les principes consultés, mais aussi ceux qui apportent un éclairage novateur et utile. Ultimement, une liste finale a été développée, celle-ci étant axée sur la pertinence au système considéré. À posteriori, une analyse de cette liste de principes, par rapport à la revue de littérature a été effectuée, afin de mettre en lumière des réflexions ultérieures à réaliser.

L'encadré ci-dessous décrit succinctement la démarche mise de l'avant. Chaque étape est explorée plus en profondeur dans les sections ci-dessous.

Démarche employée pour développer la liste de principes

6. Réalisation de l'inventaire des listes de principes existantes pertinentes.
7. Extraction et analyse de tous les principes, de façon à voir les chevauchements et particularités.
8. Développement d'une liste finale de principes axée sur la pertinence par rapport à l'IdO et la complétude par rapport aux listes consultées.
9. Analyse des chevauchements entre la liste proposée et les conclusions de la revue de littérature (Russo Garrido et al, 2017)
10. Identification des principes qui doivent être renforcés.

3.2 Inventaire des listes de principes existantes et analyse des chevauchements et différences

Les listes de principes existantes répertoriées ont été sélectionnées sur la base de deux critères :

- Leur pertinence par rapport à l'une ou plusieurs des composantes technologiques ou analytiques du système de l'IdO. Notamment, les principes au sujet des données massives, des algorithmes, de l'intelligence artificielle et des systèmes d'informations ont été considérés; et

- leur présence incontournable dans la littérature, telle que perçue par l'équipe de recherche via leurs citations et références par d'autres auteurs.

Ce repérage a été effectué avec l'appui de moteurs de recherche[8], mais surtout via des conversations-clés avec des chercheurs et intervenants dans le domaine. Quatre documents ont nourrit la réflexion de façon plus marquée, quant aux documents de base à considérer : 1) le rapport de Robert Kitchin (2016) « *Getting smarter about smart cities : Improving data privacy and data security* »; 2) l'article de Meg Leta Jones (2015) « *The Ironies of Automation Law : Tying Policy Knots with Fair Automation Principles* »; 3) le rapport de la Commission de l'éthique en sciences et technologies du Québec sur les villes intelligentes (2017); et une entrevue dans le magazine Wired (Rosenburg, 2017) avec Kate Crawford, intitulée « *Why AI is still waiting for its ethics transplant* ».

Les documents ultimement sélectionnés proviennent d'horizons variés. Certains sont des principes normatifs issus d'un consensus international, ou encore à l'échelle canadienne ou provinciale. Certains sont des déclarations et principes issus de la sphère municipale ou encore de forums ou du domaine académique. Enfin, certains sont des codes de conduite.

Le tableau ci-dessous identifie les documents sélectionnés, classés selon les composantes techniques ou thématiques auxquels ils se rapportent. Les listes de principes sont ensuite présentées dans la Section 3.3.

Tableau 1. Listes de principes considérées

Catégorie	Listes de principes
Principes normatifs relatifs à la vie privée	• Principes normatifs protection vie privée au Canada • *Fair Information Practice Principles (FIPPs)* • Lignes directrices de l'OCDE • Vie privée dès la conception • Sept principes de la protection intégrée de la vie privée de l'Ontario • Principes de la vie privée de la ville de Seattle • Législation européenne 1990 et 2018 (général)
Principes normatifs relatifs à l'IdO et la ville intelligente	• Recommandations de l'Avis de la Commission en éthique sciences et technologie du Québec sur la ville intelligente • Lignes directrices pour les villes intelligentes et équitables / *NYC IoT Guidelines*
Principes relatifs à l'intelligence artificielle[9]	• Principes de l'ASILOMAR pour l'IA bénéfique • *Fair Automation Practice Principles (FAPPs)* • Déclaration de Montréal pour un développement responsable de l'intelligence artificielle

[8] Google Scholar a surtout été utilisé, étant donné qu'il n'exclue pas, de facto, la littérature grise, qui était pressentie comme étant très centrale dans ce projet.

[9] Afin d'alimenter ultérieurement l'inventaire, la réflexion de l'IEE au sujet de l'intelligence artificielle pourrait être ajoutée à cette liste (IEEE, 2017).

Principes relatifs aux données massives[10]	• Dix règles pour la recherche responsable en données massives
Codes de conduite	• Code d'éthique et de conduite professionnelle de l'ACM • Code d'éthique de l'IEEE[11]

L'analyse de ces listes a visé à observer les chevauchements entre principes ainsi que les particularités apportées par chacune des listes. À cette étape, tous les principes ont été extraits dans un fichier Excel, ce qui a abouti à une liste totale de 80 principes distincts, ceux-ci pouvant être regroupés autour de thèmes communs. La liste intégrale de ces principes est présentée dans l'Annexe A. De cette liste, les chevauchements et les différences ont été identifiées de façon à distiller une liste de principes centraux exprimant un certain consensus mais aussi un bon niveau de complétude par rapport aux enjeux éthiques identifiés dans la littérature. Cette liste finale est présentée dans la Section 4.

3.3 Listes de principes considérées

Dans cette section seront présentées tour à tour les listes de principes ayant été considérées. Il s'agit des listes énumérées dans le Tableau 1 ci-dessus.

3.3.1 Principes normatifs concernant la protection de la vie privée au Canada

Les principes relatifs à l'équité dans le traitement des renseignements sont énoncés dans la Loi canadienne sur la protection des renseignements personnels et les documents électroniques, applicable au secteur privé (Ministère de la Justice, 2017) et résumée dans le Tableau ci-dessous.

Cette liste a été sélectionnée de par sa nature incontournable pour toute entité basée au Canada; ces principes sont la base même de la législation en matière de protection de la vie privée au Canada.

[10] Afin d'alimenter ultérieurement l'inventaire, les principes présentés dans l'article de Richards et King (2014) pourraient être ajoutés ici.

[11] Il est à noter que l'ACM et l'IEEE ont produit un code ensemble, mais celui-ci n'a pas été considéré dans l'exercice. Étant donné que l'IEEE est entrain de réviser une nouvelle version de son code individuel, il a été perçu comme plus important de se coller aux codes les plus récents, plutôt qu'à ceux réalisés en collaboration.

Tableau 2: Principes normatifs concernant la protection de la vie privée au Canada (Ministère de la Justice, 2017)

Principes	Explication
Principe 1 **Responsabilité**	Une organisation est responsable de renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous
Principe 2 **Détermination des fins de la collecte des renseignements**	Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci
Principe 3 **Consentement**	Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
Principe 4 **Limitation de la collecte**	L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.
Principe 5 **Limitation de l'utilisation, la communication et de la conservation**	Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées
Principe 6 **Exactitude**	Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés
Principe 7 **Mesures de sécurité**	Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
Principe 8 **Transparence**	Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.
Principe 9 **Accès aux renseignements personnels**	Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.
Principe 10 **Possibilité de porter plainte à l'égard du non-respect des principes**	Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisation concernée.

3.3.2 Les Fair Information Practice Principles (FIPPs) et les Lignes directrices de l'OCDE

Les *Fair Information Practice Principles* (FIPPs) et les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers de données sont à la base des principes normatifs relatifs à la vie privée au Canada (présentés ci-dessus), de même que les principes sous-tendant la majorité des lois en occident en la matière (Richards et King, 2014; Cate, 2006). Ils sont donc des principes incontournables.

Les FIPPs ont vu le jour en 1973 aux États-Unis[12]. Il s'agit de 5 principes, souvent résumés par les termes transparence, limitation dans l'utilisation, accès et correction, qualité des données et sécurité. Ces principes furent éventuellement mis à jour et bonifiés sous forme des Lignes directrices de l'OCDE.

Dans son rapport de recommandations en matière de gouvernance de la vie privée dans la ville intelligente pour la ville de Dublin, Robert Kitchin (2016) propose de baser le cadre de gouvernance sur les FIPPs, les Lignes directrices de l'OCDE et les principes de la Vie privée dès la conception (*Privacy by Design*) (Kitchin, 2016). Kitchin remarque cependant que plusieurs critiques des FIPPs et des Lignes directrices de l'OCDE affirment que ceux-ci ne parviennent pas à bien aborder la question des torts issus de l'analyse prédictive, ceux-ci émanant de l'inférence, du partage des données, de la réutilisation des données pour de nouvelles fins et de manière générale, de l'utilisation imprédictible des données dans une ère de données massives. Par ailleurs, bien que l'avis et le consentement se retrouvent par les principes mis de l'avant par FIPPs et l'OCDE, il existe une reconnaissance généralisée que ceux-ci ne sont pas réellement efficaces à ce jour dans une ville connectée (Kitchin, 2016). Nous reviendrons sur ces points dans la Section 4.

Étant donné que les normes canadiennes présentées dans la Section 3.3.1 s'inspirent en grande partie des FIPPs et des Lignes directrices de l'OCDE, il existe peu de différence entre ces documents. Cependant, ci-dessous sont identifiées les différences à noter :

- Les Lignes directrices de l'OCDE énoncent que les données à caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles seront utilisées;
- Les Lignes directrices de l'OCDE soulignent que le maître du fichier et son lieu habituel d'activité doit être transparent;
- Les Lignes directrices de l'OCDE énoncent qu'il devrait aisé pour un individu de connaitre la nature des données détenues à son sujet et les finalités principales de leur utilisation;
- Les Lignes directrices de l'OCDE apportent plus de détails sur comment la transparence vis-à-vis les individus doit être concrétisée, via des principes de participation individuelle, tel que présenté dans la Figure ci-dessous.

[12] Dans le cadre du rapport « *Records, Computers, and the Rights of CItizens* » paru en 1973, du *Advisory Committee on Automated Personal Data Systems* du gouvernement américain.

Principe de la participation individuelle

13. Toute personne physique devrait avoir le droit :

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

b) de se faire communiquer les données la concernant;

   i) dans un délai raisonnable;

   ii) moyennant, éventuellement, une redevance modérée;

   iii) selon des modalités raisonnables; et

   iv) sous une forme qui lui soit aisément intelligible;

c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet; et

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Figure 9: Principe de la participation individuelle des Lignes directrices de l'OCDE, extrait de CÉSTQ, 2017.

3.3.3 Vie privée dès la conception et Sept principes de la protection intégrée de la vie privée de l'Ontario

Le Commissaire à l'information et à la protection de la vie privée de l'Ontario a publié en 2015 un guide à l'intention des municipalités sur le sujet de la vie privée et les renseignements personnels. Le Commissaire propose sept principes aux municipalités pour aborder les enjeux en la matière. Ceux-ci sont alignés de très près avec les principes de la Vie privée dès la conception (*Privacy by Design*). Cette approche propose de placer la protection de la vie privée comme mode d'opération par défaut. Il s'agit alors d'assumer que toutes les données collectées sont privées par défaut, à moins que les citoyens proposent l'inverse. La vie privée est donc intégrée dans les spécifications de conception, l'utilisation des technologies de l'information, pratiques d'affaire, environnements physiques et infrastructure des systèmes et applications (Cavoukian, 2012; Kitchin, 2016).

La démarche ontarienne a été sélectionnée car elle présente une initiative canadienne pertinente, en lien avec les enjeux posés par l'IdO dans la ville. Elle est également basée sur la Vie privée dès la conception, une liste de principes incontournable dans le paysage des démarches visant à assurer la protection de la vie privée dans une ville intelligente, tel que mentionné par Kitchin (2016) et bien d'autres. L'utilisation de cette approche a été par ailleurs mise de l'avant par l'Union européenne, la *Federal Trade Commission* américaine, et plusieurs commissaires nationaux à la protection de la vie privée (Kitchin, 2016).

Tableau 3: Les sept principes de la protection intégrée de la vie privée de l'Ontario
(Commissaire à l'information et à la protection de la vie privée de l'Ontario, 2015)

Principe	Explication
Principe proactif et non réactif	La démarche PIVP vise à prévoir et à prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent.
Le respect de la vie privée comme paramètre par défaut	Il faut s'assurer que les données personnelles sont automatiquement protégées dans tout système informatique et toute pratique d'affaires, pour que la vie privée du particulier demeure intacte, même sans son intervention.
Intégration du respect de la vie privée au niveau de la conception	La protection de la vie privée doit faire partie intégrante de la conception et de l'architecture des systèmes informatiques et des pratiques d'affaires.
Pleine fonctionnalité – somme positive au lieu de somme nulle	Le PIVP cherche à tenir compte de tous les intérêts et objectifs légitimes selon un scénario gagnant-gagnant, qui vise à contrebalancer des intérêts apparemment opposés, comme la sécurité et le droit à la vie privée.
Sécurité de bout en bout – une protection complète pour le cycle de vie	Le PIVP s'applique à l'intégralité du cycle de vie des données concernées, du début jusqu'à la fin.
Visibilité et transparence	Le PIVP vise à assurer toutes les parties intéressées que les parties composantes et les opérations demeurent visibles et transparentes pour tous les utilisateurs et fournisseurs
Respect de la vie privée de l'utilisateur – maintenir une démarche centrée sur l'utilisateur	Avant tout, le PIVP accorde la priorité aux intérêts du particulier en proposant de solides mesures axées sur le respect de la vie privée : un paramètre par défaut, un avis adéquat et des options conviviales.

3.3.4 Principes de la vie privée de la ville de Seattle

Au terme de plusieurs mois de consultations avec des parties prenantes, la ville de Seattle a adopté six principes afférents à la vie privée en février 2015. Cette initiative a été sélectionnée car elle représente l'une des rares initiatives au niveau municipal qui vise à établir des principes de base pertinents à la gouverne de la ville intelligente.

Parmi les principes listés, quelques uns sont particulièrement complémentaires à ceux présentés dans les documents antérieurement couverts, notamment les principes véhiculant les idées suivantes :

- effectuer des évaluations d'impact sur la vie privée sur les nouveaux programmes de données;
- donner la possibilité aux citoyens de soustraire leurs données; et
- assurer que les tierces parties sous-contractées ayant accès aux données personnelles se soumettent à la politique de la vie privée de la ville.

Les principes de la ville de Seattle en matière de vie privée:

1. La valeur de la vie privée : des évaluations d'impact sur la vie privée seront réalisés sur tous les nouveaux programmes de données[13]
2. Minimisation/proportionnalité : la ville travaillera afin de collecter seulement les données nécessaires pour la fourniture/approvisionnement des services
3. Avis : la ville travaillera afin d'informer (les citoyens) de comment les données personnelles sont utilisées et donnera l'opportunité aux citoyens de soustraire leurs données aux analyses lorsque possible
4. Responsabilité : la ville respectera toutes les lois fédérales et étatiques concernant la vie privée
5. Transparence : la ville observera toutes les lois fédérales et étatiques concernant les demandes d'accès à l'information. Les tierces parties sous-contractées ayant accès aux données personnelles devront se soumettre à la politique de la vie privée de la ville
6. Précision : la ville travaillera afin de corriger les informations personnelles imprécises, lorsque possible.

La ville a par conséquent adopté un engagement à la vie privée sur la base de ces six principes, détaillant à tous les départements les pratiques afférentes à la vie privée et à la gestion des données.

(Gaughan, 2016, 33 – traduction libre)

3.3.5 Puiser de l'inspiration du côté des règlementations européennes

En 1990, la Commission de la Communauté Européenne a publié le *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* traçant la voie vers l'adoption de lois nationales parmi les États membres en la matière. Cette Directive, de même que le Règlement général sur la protection des données subséquent adopté en avril 2016 (qui sera applicable à partir de mai 2018) sont bien sûr des documents législatifs complexes, qui sont le fruit de débats et de compromis. Il n'est pas proposé ici d'en faire une analyse complète, ni de les regarder en détail, mais plutôt de prendre acte des grands principes qu'ils mettent de l'avant, plus particulièrement ceux qui abordent des enjeux jusque-là non/mal abordés.

C'est dans cet esprit que la Directive et le Règlement ont été sélectionnés dans ce projet – de par leur orientation à couvrir certains enjeux peu ou mal couverts par d'autres cadres/listes de principes. Par exemple, la Directive se penche sur l'enjeu de l'explicabilité des prises de décision automatisées et propose l'indépendance de supervision – le fait qu'un organe externe puisse auditer la gestion et l'utilisation des données – et le recours individuel en cas de tort. Le tableau ci-dessous présente un extrait de ces principes.

[13] Cet engagement exige également une évaluation d'impact sur la vie privée et une analyse de seuils de privacité (*privacy threshold)* pour tout nouveau programme de collecte de données (Gaughan, 2016).

Tableau 4 : Principes de la Directive européenne de 1990

Principes de la Directive européenne de 1990		
1	Limite des objectifs	Les données devraient être utilisées pour des fins spécifiques et subséquemment analysées ou communiquées seulement si ceci n'est pas incompatible avec les fins du transfert initial. Lorsque les données sont transférées pour des fins de marketing, les sujets des données devraient être en mesure de soustraire ses données si souhaité
2	Qualité des données et proportionalité	Les données devraient être précises et lorsque nécessaire maintenues à jour. Les données devraient être adéquates, pertinentes et non excessives en relation avec les objectifs pour lesquelles elles ont été transférées ou traitées
3	Transparence	Les individus devraient recevoir de l'information concernant les objectifs visés par le traitement des données et l'identité du contrôleur des données (…) et toute autre information nécessaire pour assurer la l'équité.
4	Sécurité	Les mesures de sécurité techniques et organisationnelles devraient être prises par le contrôleur de données, en fonction des risques présentées dans le traitement des données (…)
5	Accès, rectification et opposition	le sujet des données devrait avoir le droit d'obtenir une copie des données en lien avec lui/elle qui sont traitées et le droit de rectification lorsque les données ne sont pas précises. Dans certaines situations il devrait être en mesure de s'opposer au traitement de données en lien avec lui/elle.
6	Restriction sur les transferts ultérieurs	Il devrait être permis au récepteur des données initialement transférées de faire des transferts de données ultérieurs seulement dans les cas où le second récepteur (celui recevant le transfert ultérieur) est également sujet à des règles permettant un niveau adéquat de protection
7	Données sensibles	Lorsque des catégories sensibles de data sont impliquées (concernant les origines raciaux, ethniques, les opinions politiques, croyances religieuses, convictions philisophiques et éthiques (…) ou la santé et la vie sexuelle) des mesures de sécurité additionnelles devraient être en place, tel que le requis que les sujets des données donnent leur accord explicite pour le traitement des données.
8	Décision individuelle automatisée	Lorsque l'objectif du transfert est pour prendre une décision automatisée, l'individu devrait avoir le droit de connaître la logique impliquée dans la décision et d'autres mesurer devraient être prises pour sauvegarder l'intérêt légitime de l'individu.
Principes de mise en application accolés à la Directive		
1	Supervision indépendante	Les entités qui traitent des données personnelles ne sont pas seulement responsables mais aussi sujettes à une supervision indépendante, ayant l'autorité pour auditer les systèmes de traitement des données, investiguer les plaintes provenant d'individus et mettre en place des sanctions pour la non-conformité
2	Recours individuel	Les individus doivent avoir le droit de poursuivre légalement les contrôleurs de données et entités impliquées dans le traitement des données qui ne respectent pas la loi. Ils doivent avoir decours à la cour et aux investigations des agences gouvernemantales (...)

Le Règlement comprend quant à lui les éléments novateurs suivants, pertinents au système de l'IdO :

- Rendre le consentement explicite et positif
- Droit à l'effacement (lorsque possible)
- Droit à la portabilité des données personnelles
- *Privacy by design* par défaut
- Notification en cas de fuites de données
- Nomination d'un délégué à la protection des données pour les organismes publics ou privés
- Évaluation d'impact obligatoire pour toutes les activités qui peuvent avoir des conséquences importantes en matière de vie privée
- Encouragement pour le développement de codes de conduite (European Parliament, 2016; Wikipedia, 2017)

3.3.6 Avis de la Commission d'éthique sciences et technologie du Québec sur la ville intelligente

En juin 2017, la Commission d'éthique en sciences et technologie du Québec a adopté un avis intitulé « La ville intelligente au service du bien commun : Lignes directrices pour allier l'éthique au numérique dans les municipalités du Québec » (CÉSTQ, 2017). Ce document vise à proposer des lignes directrices pour promouvoir le développement de villes intelligentes au service du bien commun, qui allient de façon harmonieuse l'éthique avec le déploiement de nouvelles technologies. Ce document a été sélectionné pour alimenter la réflexion, vu son importance centrale dans la réflexion sur les villes intelligentes et leurs technologies au Québec.

De manière générale, la Commission propose d'orienter les politiques relatives à la ville intelligente en fonction des principes éthiques suivants :

- maximiser les bénéfices sur le plan du bien commun;
- éviter ou réduire le plus possible les préjudices potentiels portés à la dignité, à la vie privée et à la vie démocratique;
- assurer une distribution équitable des bénéfices et des préjudices possibles entre les acteurs concernés;
- s'assurer que les bénéfices attendus sont toujours supérieurs aux inconvénients, dont les coûts (CÉSTQ, 2017).

La Commission clos son avis en énonçant des valeurs et des principes à respecter, tel que présenté ci-dessous. Il est cependant à noter que bon nombre de valeurs et principes traitent davantage de la ville intelligente que de l'IdO de façon spécifique. Par ailleurs, plusieurs éléments listés ont une résonance avec des principes listés précédemment. Cependant, certains sont novateurs et fortement pertinents, notamment ceux afférents à:

- la démocratie (en particulier le principe de promotion de la participation citoyenne dans les décisions et usages);
- le bien commun (en particulier l'autonomie de la sphère publique, la primauté de l'intérêt public, l'inclusion, la non socialisation des coûts pour des services privés); et
- l'équité (en particulier le traitement juste, la justice spatiale (territoriale), l'inclusion numérique).

Les valeurs et principes recommandés par la CÉSTQ sont présentés à l'Annexe B.

3.3.7 Lignes directrices pour les villes intelligentes et équitables lancées par NYC

Les Lignes directrices pour les villes intelligentes et équitables ont été d'abord lancées en 2016 par la ville de New York, originalement sous le nom de « *NYC Guidelines for the Internet of Things* ». Elles ont ensuite été signées par plus de 30 villes à travers le monde, dont la ville de Paris. Ces Lignes directrices ont pour objectif d'aider les administrations municipales à comprendre les risques potentiels associés avec les déploiements de l'IdO, promouvoir une approche harmonisée pour leurs déploiements d'IdO, donner de la transparence au secteur privé sur l'approche de la ville par rapport à l'IdO et informer le public. Ces Lignes directrices ont été sélectionnées pour leur résonnance internationale et la pertinence de leur sujet central. Elles s'appuient par ailleurs sur les meilleures pratiques et les leçons apprises de plus de 50 villes à travers le monde (NYC, sans date).

Les Lignes directrices sont un mélange de principes, de mesures opérationnelles et de pratiques de gestion. Elles traitent d'enjeux éthiques, mais aussi de saine gouvernance des infrastructures. Bien que leur intitulé mette l'emphase sur la ville intelligente, elles sont en réalité très centrées sur le déploiement de l'IdO. Les lignes directrices sont articulées autour de 5 principes, présentés ci-dessous et en détail dans l'Annexe C.

Résumé des Lignes directrices pour les villes intelligentes et équitables

1. **Vie privée et transparence** : Les déploiements de l'IdO dans la ville doivent protéger et respecter la vie privée des résidents et visiteurs. La ville s'engage à être ouverte et transparente par rapport au « qui, quoi, où, pourquoi et comment » de la collecte de données, la transmission, le traitement et l'utilisation.
2. **Gestion des données** : Les données sont au centre de tout système d'IdO. Nous assurerons que l'IdO et les données en temps réel sont collectées, stockées, vérifiées et rendues accessibles de manière à maximiser les bénéfices pour la collectivité.
3. **Infrastructure :** Les équipements de l'IdO, les réseaux et les infrastructures devraient être déployées, utilisées, maintenues et mises à disposition d'une manière efficace, responsable et sécuritaires, afin de maximiser l'intérêt public.
4. **Sécurité :** les systèmes d'IdO devaient être conçus et opérés avec la sécurité au centre de son action, afin de protéger le public, assurer l'intégrité de ses services et être résilient aux attaques.
5. **Opérations et durabilité :** tous les déploiements d'IdO devraient être structurés afin de maximiser les avantages pour le public et assurer la durabilité financière, opérationnelle et la durabilité environnementale.

(NYC, 2017 – traduction libre)

3.3.8 Principes ASILOMAR pour l'IA bénéfique

Les 23 principes D'ASILOMAR ont vu le jour en 2017, suite à la Conférence *Beneficial Artificial Intelligence,* organisée par le *Future of Life Institute*. Cet évènement rassemble des acteurs du monde académique et industriel s'intéressant à l'intelligence artificielle (IA), depuis la perspective de la technique, mais aussi de l'économie, du droit, de l'éthique et de la philosophie[14]. Ils sont listés parmi les cadres de principes qui ont émergé récemment au sujet de l'IA et qui sont à prendre en compte (Crawford dans Rosenburg, 2017).

Les principes visent à identifier « ce que la société devrait faire pour gérer, au mieux, l'intelligence artificielle dans les prochaines décennies » (Future of Life Institute, 2017). Sur la base de la littérature et en particulier les plus récents rapports sur le sujet émanant du monde académique, politique et sans but lucratif[15], une première ébauche de la liste a été développée par les organisateurs de la conférence en amont de l'évènement. Cette liste a été ouverte à commentaires et bonifications par les participants de la conférence avant et pendant l'évènement, via des ateliers de discussions pour cette fin spécifique et une enquête généralisée. Seuls les principes ayant reçu l'approbation de 90% des participants furent

[14] Il est à noter que plusieurs des acteurs affiliés à cette initiative sont très critiques du développement de l'AI et croient qu'elle comporte en son sein un potentiel de destruction de l'humanité (tel que peut être perçu dans certains des principes mis de l'avant). Ceci est contraire à la position des acteurs qui promeuvent par exemple la Déclaration de Montréal, portant également sur le sujet de l'AI, mais qui perçoivent cette dernière comme un développement technique à baliser (Communication personnelle, 2017)

[15] Par exemple le *Stanford 100 Year report*, les récents rapports pour la Maison Blanche ou le rapport *Materials from partnership on AI* (ASILOMAR, 2017).

conservés pour la version finale – qui se veut l'ouverture d'un dialogue vers une réflexion évolutive et perfectible.

Ces principes traitent de sujets dignes d'intérêt, dont :

- Assurer que la sécurité des systèmes soit vérifiable
- Transparence de l'échec d'un système
- Ne pas miner les processus sociaux et civique.

Ces principes sont présentés ci-dessous (des omissions ont été réalisées pour des fins de communication efficace – les principes dans leur forme intégrale et originale se trouvent à l'Annexe D).

Tableau 5: Principes d'ASILOMAR pour l'IA bénéfique

Thème	Principes
	Enjeux de recherche
Le but de la recherche	Le but de la recherche devrait être de créer non pas de l'intelligence non dirigée, mais de l'intelligence bienfaitrice Les investissements en IA devraient être accompagnés par de la recherche pour assurer leur utilisation bénéfique
Lien entre la science et la politique	Il devrait y avoir un échange constructif et sain entre les chercheurs en IA et les décideurs politiques
Culture de recherche	Une culture de coopération, confiance et transparence devrait être promue entre les chercheurs et développeurs de IA.
Éviter une course	Les équipes qui développent des systèmes IA devraient coopérer activement pour éviter « de tourner les coins ronds » en ce qui concerne les garanties de sécurité.
	Valeurs et éthique
Sécurité	Les systèmes IA devraient être sécuritaires (*safe and secure*) à travers leur vie opérationnelle et ce, de manière vérifiable là où applicable et faisable.
Transparence de l'échec	Si un système IA provoque des dommages (*causes harm*), il devrait être possible d'expliquer pourquoi.
Transparence judiciaire	Toute implication d'un système autonome dans une prise de décision judiciaire devrait produire une explication satisfaisante et vérifiable par une autorité humaine compétente.
Responsabilité	Les développeurs et bâtisseurs de systèmes avancés IA sont les parties prenantes dans les implications morales de leur utilisation, mauvaise utilisation et actions, avec une responsabilité et opportunité pour façonner ces implications.
Alignement des valeurs	Des systèmes hautement autonomes devraient être élaborés afin que leurs buts et comportements puissent être alignés avec les valeurs humaines dans leurs opérations.
Valeurs humaines	Les systèmes IA devraient être élaborés et opérés de façon à être compatible avec les idéaux de dignité humaine, droits, libertés et diversité culturelle.
Vie privée personnelle	Les personnes devraient avoir le droit d'accéder, gérer et contrôler les données qu'elles génèrent, vu le pouvoir des systèmes IA pour analyser et utiliser ces données.
Liberté et vie privée	L'application de l'IA aux données personnelles ne devrait pas

	déraisonnablement entraver la liberté réelle ou perçue des individus
Bénéfices partagés	Les technologies IA devraient apporter des avantages et « empower » autant de gens que possible
Prospérité partagée	La prospérité économique créée par IA devrait être partagée de façon large, afin que toute l'humanité puisse en bénéficier
Contrôle humain	Les humains devraient choisir comment et si ils délègueront des décisions aux systèmes IA, afin d'accomplir des objectifs choisis par les humains.
Non-subversion	Le pouvoir conféré par le contrôle de systèmes IA très avancés devrait respecter et améliorer, plutôt que miner, les processus sociaux et civiques desquels le bien-être de la société dépend.
La course aux armes IA	Une course aux armes autonomes létales IA devrait être évitée.
	Enjeux à long terme
Prudence par rapport aux capacités	Étant donné l'absence d'un consensus, nous devrions éviter des postulats forts sur les limites les plus élevées par rapport au futur des capacités de l'IA.
Importance	L'IA avancée pourrait représenter un changement profond dans l'histoire de la vie sur la terre et devrait être planifié et gérer avec beaucoup de soin et de ressources.
Risques	Les risques posés pas les systèmes IA, spécialement les risques catastrophiques et existentiels, devraient être sujets à la planification et la mitigation des efforts, proportionnels à leur impact attendu.
Auto-amélioration récurrente	Les systèmes élaborés pour s'auto-améliorer et s'auto-reproduire de manière récurrente et d'une façon qui pourrait mener à améliorer rapidement la qualité ou la quantité devrait être sujet à des mesures de sécurité et contrôle strictes.
Le bien commun (Future of Life Institute, 2017)	La super-intelligence devrait seulement être développée pour être au service d'idéaux partagés de manière élargie et pour le bénéfice de toute l'humanité plutôt qu'un état ou une organisation.

3.3.9 Les Fair Automation Practice Principles

Les *Fair Automation Practice Principles* (FAPPs) on été proposés par l'universitaire Meg Leta Jones (2015). Il s'agit de principes pour encadrer le développement des objets autonomes – depuis les systèmes de prise de décision autonome, aux véhicules autonomes. Ces principes sont inspirés des FIPPs et de plusieurs autres documents de principes fondateurs, tels les principes de la vie privée de Richards et King (2014) et de l'éthique des interactions humain-robot de Riek et Howard (2014). Cette liste de principe a été sélectionnée en raison de sa résonance dans la littérature, ainsi que du fait qu'elle bâtit et s'inspire à même d'autres cadres existants ayant été identifiés comme étant pertinents, dans le cadre de ce rapport ou encore de la revue de la littérature qui le précède.

Il s'agit de 7 principes qui complémentent les pratiques de design existantes, qui prennent acte de l'utilisation réelle des objets et aident à identifier les endroits où une expertise additionnelle serait nécessaire (Jones, 2015, 121). Jones souligne que les principes d'automation ne peuvent pas être définis en isolation; ils doivent être collectivement délibérés et développés par des concepteurs, gestionnaires, utilisateurs, investisseurs, des politiques, des éthiciens et des juristes. Les principes proposés sont donc une invitation au dialogue multipartite, plutôt qu'une liste finale. Le Tableau 6 ci-dessous résume ces principes.

Ces principes apportent notamment les éléments suivants à la réflexion :

- l'évaluation du risque pour l'humain, avec une reconnaissance des limites de nos outils actuels;
- La transparence des systèmes;
- Assurer que la défaillance des systèmes soit non surprenante, non silencieuse et non irrésoluble;
- Tester les impacts discriminatoires;
- Réfléchir aux impacts sur les valeurs sociales élargies; et
- Inventorier les comportements prédictibles et imprédictibles.

Tableau 6: *Les Fair Automation Practice Principles* (Jones, 2015)

Principes
Principe 1 - Risque : Les systèmes automatisés ne devraient pas être déployés sans une évaluation des risques pour l'humain dans la boucle (*human in the loop*) ou les humains affectés par la boucle. Les évaluations ne doivent pas être laissées seulement aux entreprises, innovateurs et développeurs. Nous devons également prendre acte du fait que les outils actuels, tels l'évaluation de risque, les analyses coûts-avantages, la modélisation plus prédictive, sont limitées – ceux-ci sont centrés sur les risques connus à court terme.
Principe 2 – Transparence : Les systèmes automatisés devraient être compréhensibles et supporter la connaissance situationnelle, via une transparence. Un système de boîte noire est toujours un mauvais design. Lorsqu'un opérateur ne sait ce que le système fait, la reconnaissance des erreurs, l'intervention, et la résolution sont gourmandes de temps et coûteuses, sinon impossibles. Citron et Pasquale ont argumenté en faveur de l'accès aux jeux de données, au code de source, aux notes des programmeurs décrivant les variables et les corrélations mobilisées – « *anything required to be able to meaningfully assess systems whose predictions change pursuant to AI logic* » (Jones, 2015, 125)
Principe 3 – Erreurs et limitations : Les défaillances des systèmes automatisés ne devraient pas être surprenantes, silencieuses ou irrésolubles. La connaissance situationnelle, la charge mentale, la dégradation des habiletés et les biais dans l'automatisation devraient être considérés lorsqu'on conçoit la détection des erreurs et lorsqu'on considère les limitations. Les travaux de Citron sur les systèmes d'assurance sociale aux États-Unis révèlent un grand nombre d'erreurs sans aucun bon moyen d'alerter les opérateurs et résoudre les problèmes dans un délai convenable.
Principe 4 – Diversité et discrimination : Les systèmes automatisés devraient réfléchir sur les biais et les choix durant le design et tester les impacts discriminatoires potentiels y compris par rapport à des utilisateurs diversifiés.
Principe 5 – Situation sensibles : Les systèmes automatisés devraient prendre en compte les situations sensibles et les préférences informationnelles des humains dans la boucle. Les informations privées ou celles relatives à des populations vulnérables devraient être évaluées avec le niveau approprié de soin et d'expertise.
Principe 6 - Comparaison de l'humain-machine : La conception et la mise en œuvre des systèmes automatisés devraient identifier/localiser l'humain dans la boucle et réévaluer l'impact du système sur l'humain et ses valeurs sociales élargies. Nous devons considérer l'humain est imparfait. Une discussion sur quelles décisions critiques doivent être faites par les humains (et pourquoi) et comment limiter les biais de l'automatisation et les « tampons moraux » (*moral buffers*) dans ces situations seraient une contribution utile pour accompagner le développement de l'automatisation.

Principe 7 – Prédictibilité : Les systèmes automatisés devraient être initialement et continuellement inventoriés pour des comportements prédictibles et imprédictibles.

3.3.10 Déclaration de Montréal pour un développement responsable de l'intelligence artificielle

La Déclaration de Montréal pour un développement responsable de l'intelligence artificielle a vu le jour en novembre 2017, lors de la clôture du Forum sur le développement socialement responsable de l'intelligence artificielle. Développée par un groupe d'organisateurs du Forum, comprenant des chercheurs de diverses disciplines en lien avec l'IA, la Déclaration vise à promouvoir le dialogue entre le public, les experts et les représentants des pouvoirs publics sur le sujet de l'intelligence artificielle au Québec (Forum IA Responsable, 2017).

La déclaration, identifie sept valeurs: bien-être, autonomie, justice, vie privée, connaissance, démocratie et responsabilité. Pour chacune d'entre elles, une série de questions sont proposées, qui visent à explorer la relation de la valeur avec le développement de l'IA. Pour chaque valeur, un principe général est également proposé, celui-ci ne répondant toutefois pas directement aux questions soulevées. La déclaration est présentée dans son intégralité dans l'Annexe E.

La déclaration a été sélectionnée par la pertinence de son origine géographique et l'importance de Montréal dans l'échiquier du développement de l'IA à l'échelle internationale.

Tableau 7: Extrait de la Déclaration de Montréal

Valeur et principe proposé	Questions
Bien-être **Principe proposé :** Le développement de l'IA devrait ultimement viser le bien-être de tous les êtres sentients.	**Questions :** • Comment l'IA peut-elle contribuer au bien-être ? • Est-il acceptable qu'une arme autonome puisse tuer un être humain ? Un animal? • Est-il acceptable qu'une IA contrôle un abattoir ? • (…)
Autonomie **Principe proposé :** Le développement de l'IA devrait favoriser l'autonomie de tous les êtres humains et contrôler, de manière responsable, celle des systèmes informatiques.	• Comment l'IA peut-elle contribuer à l'autonomie des êtres humains? • Faut-il lutter contre le phénomène de capture de l'attention dont s'accompagnent les avancées de l'IA ? • Faut-il s'inquiéter de ce que des humains préfèrent la compagnie des IA à celle d'autres humains ou d'animaux ? • (…)
Justice **Principe proposé:** Le développement de l'IA devrait promouvoir la justice et viser à éliminer les discriminations, notamment celles liées au genre, à l'âge, aux capacités mentales et	• Comment s'assurer que les bénéfices de l'IA soient accessibles à toutes et à tous? • Faut-il lutter contre la concentration du pouvoir et de la richesse au sein d'un petit nombre d'entreprises en IA? • Quelles sont les discriminations que l'IA pourrait créer ou exacerber ? • Le développement de l'IA devrait-il être neutre ou chercher à réduire les inégalités économiques et sociales?

physiques, à l'orientation sexuelle, aux origines ethniques et sociales et aux croyances religieuses.	• Quels types de décisions de justice pourrait-on déléguer à une IA?
Vie privée **Principe proposé:** Le développement de l'IA devrait offrir des garanties sur le respect de la vie privée et permettre aux personnes qui l'utilisent d'accéder à leurs données personnelles ainsi qu'aux types d'informations que mobilise un algorithme.	• Comment l'IA peut-elle garantir le respect de la vie privée ? • Nos données personnelles nous appartiennent-elles et devrait-on avoir le droit de les effacer? • Devrait-on savoir à qui nos données personnelles sont transmises et, plus généralement, qui les utilise ? • Est-il contraire aux règles d'éthique ou d'étiquette qu'une IA réponde à votre place à vos courriels ? • Qu'est-ce qu'une IA pourrait faire en votre nom?
Connaissance **Principe proposé:** Le développement de l'IA devrait promouvoir la pensée critique et nous prémunir contre la propagande et la manipulation.	• Le développement de l'IA fait-il courir un risque à la pensée critique? • Comment minimiser la circulation de fausses nouvelles ou d'informations mensongères? • Les résultats des recherches (positifs ou négatifs) en IA doivent-ils être disponibles et accessibles? • (…)
Démocratie **Principe proposé:** Le développement de l'IA devrait favoriser la participation éclairée à la vie publique, la coopération et le débat démocratique.	• Faut-il contrôler institutionnellement la recherche et les applications de l'IA? • Dans quels domaines est-ce le plus pertinent? • Qui devrait décider - et selon quelles modalités - des normes et valeurs morales déterminant ce contrôle ? • (…)
Responsabilité **Principe proposé:** Les différents acteurs du développement de l'IA devraient assumer leur responsabilité en œuvrant contre les risques de ces innovations technologiques. (Forum AI Responsable, 2017)	• Qui sont les acteurs responsables des conséquences du développement de l'IA? • Comment définir un développement progressiste ou conservateur de l'IA ? • Comment réagir devant les conséquences prévisibles sur le marché du travail? • (…)

3.3.11 Dix règles pour la recherche responsable en données massives

Les dix règles pour la recherche responsable ont été proposées par le *Council for Big Data, Ethics, and Society,* un groupe de 20 chercheurs reconnus internationalement, issus des sciences sociales, naturelles et informatiques. Les règles sont en partie inspirées des règles de biologie computationnelle PLOS, les premières 5 règles développées afin de réduire les possibilités des dommages (*harm*) résultant des pratiques des recherches en données massives. L'importance du *Council for Big Data, Ethics, and Society* dans le paysage de l'analyse critique des données massives et le nombre de chercheurs de hauts calibre ayant apposé leur signature aux Dix règles en fait un document incontournable.

En termes des idées avancées, elle apporte plusieurs éléments très utiles à la présente réflexion, notamment :

- la notion que la vie privée n'est pas binaire. La vie privée est contextuelle, situationnelle et non réductible à l'opposition public vs. privé. La vie privée ne concerne pas seulement les individus, mais s'étend également aux groupes;
- Il est impératif de protéger la réidentification des données;
- Les choix difficiles en matière éthique devraient être débattus et perçus comme faisant partie entière du travail à aborder;
- Organiser/développer les données et les systèmes pour permettre l'audit de ceux-ci; et
- S'impliquer pour comprendre et prendre part aux conséquences plus larges des données et des pratiques d'analyse.

Dix règles pour la recherche responsable en données massives (résumé)

1. Reconnaître que les données sont des personnes et elles peuvent faire du tort : les données représentent des personnes et ont un impact sur elles.
2. Reconnaître que la vie privée est plus qu'une valeur binaire : la vie privée est contextuelle et situationnelle, pas réductible à une donnée binaire public/privé. La vie privée va également au-delà des individus et s'étend aux groupes. Ceci est particulièrement le cas pour des communautés qui ont fait l'objet historiquement de politiques discriminatoires axées sur les données, comme la pratique du redlining.
3. Se prémunir contre la réidentification des données (…). Identifier les vecteurs possibles de la réidentification des données (…).
4. Pratiquer le partage éthique des données.
5. Considérer les forces et les limitations de vos données; données massives ne riment pas automatiquement avec meilleures données.
6. Débattre des choix difficiles éthiques: plutôt qu'un problème, le manque de solutions claires et de protocoles de gouvernance devrait être compris comme une aspect inhérent que les chercheurs devraient aborder dans leur travail.
7. Développer un code de conduite pour une organisation, communauté de recherche ou industrie : comme un moyen de cimenter la pratique quotidienne.
8. Concevoir les données et les systèmes pour qu'ils soient auditables.
9. S'impliquer pour comprendre les conséquences plus larges sur la société de la collecte des données et des pratiques d'analyses.
10. Savoir quand briser ces règles : en cas d'urgence

(Zook et al, 2017 – traduction libre)

3.3.12 Le code d'éthique et de conduite professionnelle de l'ACM

L'ACM (*Association for Computing Machinery*) a publié son premier code d'éthique et de conduite professionnelle en 1992 et procède actuellement à sa mise à jour (date attendue 2018). Le code est destiné à appuyer les professionnels de l'informatique. Le code est séparé en 4 sections. Section 1 traite de considérations fondamentales éthiques; Section 2 aborde les considérations de responsabilité professionnelle; Section 3 aborde le rôle des individus ayant des positions de leadership dans le milieu du travail ou dans une capacité professionnelle. Finalement, les principes pour la conformité avec le code sont couverts dans la Section 4.

La version 2018 du code est résumée dans le Tableau ci-dessous et présentée dans son intégralité dans l'Annexe F. Il apporte plusieurs points intéressants à la réflexion. D'une part, le niveau de détail donné

par rapport à chacun des principes et la façon dont ceux-ci sont déclinés dans le quotidien de praticiens dans le domaine de l'information, apporte des précisions pratiques potentiellement utiles. Par ailleurs, le code souligne les aspects suivants:

- Assurer que les équipements/approches informatiques soient utilisés d'une façon socialement responsable par autrui.
- Prioriser l'honnêteté et la confiance, en particulier en ce qui concerne la manipulation/création de données
- Prendre action afin de ne pas discriminer via l'analyse des données.

Le Code de l'ACM a été sélectionné car il est cité à plusieurs reprises comme étant un document de référence en ce qui concerne des démarches concrètes pour aborder les enjeux éthiques dans les professions de l'ingénierie et les sciences informatiques.

General Moral Principles (en anglais)

A computing professional should…

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should give consideration to whether the products of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible.

1.2 Avoid harm.

In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified death, unjustified loss of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. A computing professional should be fair and not make deliberately false or misleading claims and should provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and scientific misconduct are similarly violations of the Code.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and equal justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ACM policy.

1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.

1.6 Respect privacy.

"Privacy" is a multi-faceted concept and a computing professional should become conversant in its various definitions and forms.

This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.

Only the minimum amount of personal information necessary should be collected in a system. The retention and

disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent of the individual(s). When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in any one of those collections in isolation.

1.7 Honor confidentiality.

Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

(ACM, version actuelle pour 2018)

3.3.13 Code d'éthique de l'IEEE

L'IEEE (*Institute of Electrial and Electronics Engineers*) est l'organisation professionnelle technique de référence dans le domaine technologique (IEEE, 2017b) ayant vu le jour d'abord aux États-Unis. Elle se présente comme la « voix » pour le génie, les sciences informatiques et la technologie de l'information à travers le monde – il est cependant à noter que ses origines américaines sont toujours très présentes, en termes de d'adhésions et orientations politiques.

Le code d'éthique de l'IEEE couvre 10 principes. Ceux-ci sont intéressants car ils sont formulés pour être mis en application par des professionnels en technologies informatiques. Ils couvrent par ailleurs des sujets pertinents et non couverts par d'autres listes de principes :

- la responsabilité d'informer rapidement les éléments qui pourraient mettre en danger le public ou l'environnement
- d'être honnête et réaliste lorsqu'on émet des affirmations ou estimés basés sur des données.

Le Code de l'IEEE a été sélectionné car il est cité à plusieurs reprises comme étant un document de référence en ce qui concerne des démarches concrètes pour aborder les enjeux éthiques dans les professions de l'ingénierie et les sciences informatiques.

Code d'éthique de l'IEEE (résumé)

1. Accepter la responsabilité de prendre des décisions qui favorisent la sécurité, la santé et le bien-être du public et divulguer promptement les facteurs qui pourraient mettre en danger le public et l'environnement;
2. Éviter les conflits d'intérêt réels ou perçus lorsque possible et les divulguer aux parties affectées le cas échéant;
3. Être honnête et réaliste lors de la présentation des conclusions et estimés basés sur les données disponibles;
4. Rejeter la corruption sous toutes ses formes;
5. Améliorer la compréhension de la technologie; son application appropriée et ses conséquences potentielles;
6. Maintenir et améliorer les compétences techniques et réaliser des tâches technologiques pour les autres seulement si l'on est qualifié par formation ou par expérience, ou suite à une divulgation complète des limitations pertinentes;
7. Rechercher, accepter et offrir des critiques honnêtes du travail technique, afin de reconnaître et corriger les erreurs et donner crédit à la contribution des autres;
8. Traiter de manière juste toutes les personnes et ne pas prendre part à des actes de discrimination basés sur la race, la religion, le genre, l'handicap, l'âge, l'origine national, l'orientation sexuelle, l'identité de genre et l'expression de genre;
9. Ne pas blesser les autres, leur propriété, leur réputation ou leur emploi en prononçant des faussetés ou réalisant des

actions malicieuses;

10. Appuyer les collègues dans leur développement professionnel et les appuyer dans leur respect de ce code d'éthique.

(IEEE, 2017 – traduction libre)

4 Liste de principes proposée

La liste finale de principes proposée dans le cadre de ce rapport a été développée en prenant acte de tous les principes couverts dans la Section 3.3. Ces principes ont ensuite été classifiés, résumés et distillés afin d'en arriver à une liste finale, avec les critères suivants en tête :

- Complétude : couvrir un maximum de thèmes identifiés dans les listes de principes consultés ;
- Pertinence : tous les thèmes directement pertinents à la gestion des enjeux éthiques et les différentes composantes techniques du système de l'IdO[16] ;
- Du général au spécifique : Identifier un nombre restreint de principes généraux et décliner, sous ceux-ci, des principes plus spécifiques.

Il est bien sûr à noter que le cadre proposé constitue une proposition de base. Il devra être appelé à évoluer et à se renforcer via la consultation/vérification d'autres documents de référence, via la délibération au sein de la ville de Montréal, ainsi que des consultations plus élargies avec des parties prenantes.

Le tableau ci-dessous présente les grands principes proposés. Ceux-ci peuvent ensuite être déclinés en sous-principes, ou principes spécifiques, tel que présenté dans l'Annexe G. La majorité des formulations proposées ci-dessous proviennent des Normes canadiennes sur la protection des données personnelles (pour les sujets afférents à la vie privée et la transparence), l'Avis sur la ville intelligente de la CÉSTQ (pour les sujets afférents au bien commun, la démocratie et la participation citoyenne, l'autonomie des pouvoirs publics) et les Lignes directrices pour les villes intelligentes et équitables.

Cette liste vise à rassembler les principes les plus importants pour orienter l'analyse et la gestion des enjeux éthiques et sociaux associés au système technologique et analytique de l'IdO dans la ville. Ils rassemblent les thématiques émanant de 13 listes/cadres existants, pertinents au système étudié, à l'exception du dernier, celui relatif à la Liberté. Tel que sera expliqué en détail dans la Section 4.1, celui-ci a été ajouté étant donné que cet enjeu, identifié dans la revue de littérature (Russo Garrido et al, 2017), n'est pas abordé de manière complète par les listes de principes consultées.

.

[16] Cependant, les principes traitant de la bonne gouvernance générale de l'IdO (en termes de maintien d'infrastructure, d'opérationnalité, etc.), ont été évacués de l'exercice.

Tableau 8: Liste de 11 principes

Thème	Principe
Bien commun	Assurer que l'IdO soit au service du bien commun et de la recherche d'un optimum social.
Démocratie et participation citoyenne	Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique
Vie privée	Protéger et respecter la vie privée* des citoyens
Transparence	Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation
Sécurité	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Bonne gestion des données	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Évaluations et conséquences	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeurs sociales élargies
Équité et inclusion	Mettre tous les moyens en œuvre pour que le traitement accordé tous soit juste et impartial. Éviter le profilage, la discrimination et le renforcement des inégalités pour développer un projet inclusif
Autonomie des pouvoirs publics	Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés
Systèmes explicables	Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision, ainsi qu'une explication des données utilisées (quelle donnée, quelle source, comment est-elle mobilisée)
Liberté	Assurer que le citoyen puisse préserver son sentiment de liberté

* Le concept de la vie privée fait l'objet de nombreux débats quant à sa définition. Ici, le terme est entendu comme la liberté des individus vis-à-vis toute intrusion physique, toute interférence dans leur vie personnelle et des entraves à leur capacité de contrôle de l'accès et de l'utilisation de leurs informations personnelles.

Les principes spécifiques, qui peuvent être déclinés sous chacun des grands principes listés ci-dessus, sont présentés dans l'Annexe G. L'Annexe présente par ailleurs, de manière transparente, l'origine de la formulation des grands principes proposés (de quelle liste, cadre ou code ils proviennent) ainsi que les listes de principes consultées qui coïncident sur différents sujets.

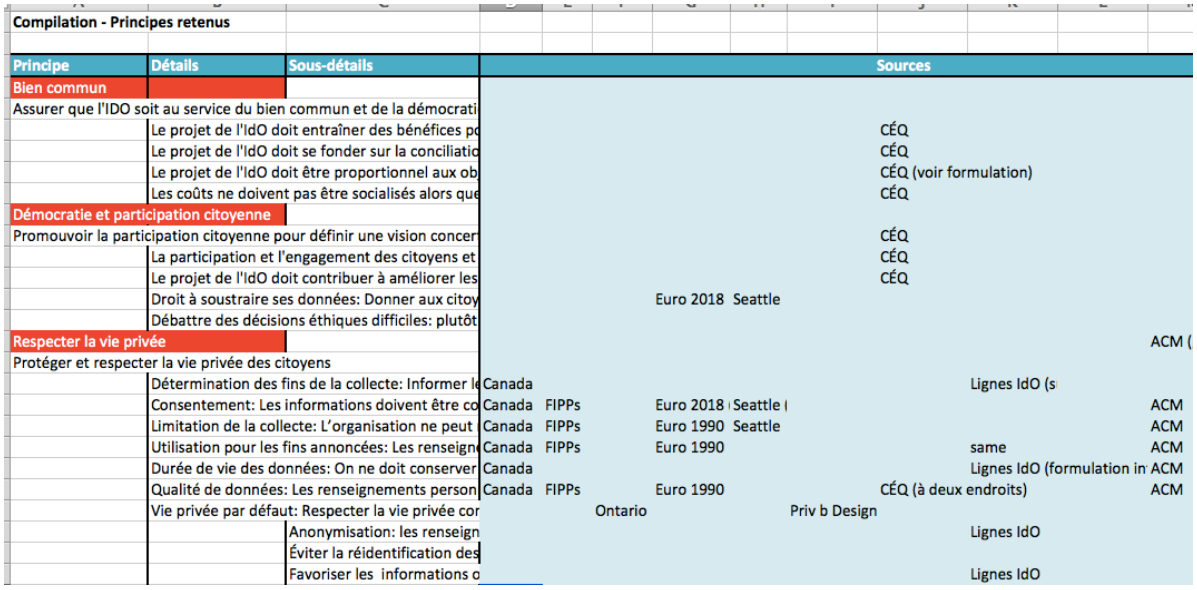
Une approche exhaustive et bien documentée a été privilégiée pour la sélection des principes spécifiques – cette sélection a donc été effectuée avec l'objectif d'arriver à un nombre maximal de principes spécifiques pertinents au système de l'IdO dans la ville, en évacuant les redondances possibles entre des principes spécifiques trop semblables. Il appartiendra à l'équipe de la Ville de décider les principes finaux retenus et leur niveau de spécificité souhaité.

Un extrait de l'Annexe G est présenté à la Figure 12, mettant en relief les grands principes et les principes spécifiques répertoriés. Cette Annexe est à nouveau présentée à la Figure 13, cette fois-ci mettant en relief les sources appuyant chacun des principes répertoriés.

Compilation - Principes retenus

Principe	Détails	Sous-détails
Bien commun		
Assurer que l'IDO soit au service du bien commun et de la démocratie (inspiré de CÉSTQ)		
	Le projet de l'IdO doit entraîner des bénéfices pour la collectivité (CÉSTQ) (inspiré Asilomar, FAPPs)	
	Le projet de l'IdO doit se fonder sur la conciliation des valeurs, perspectives, intérêts pluriels présents dans la société civile et sur la recherche	
	Le projet de l'IdO doit être proportionnel aux objectifs visés (CÉSTQ)	
	Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (équité)(CÉSTQ)	
Démocratie et participation citoyenne		
Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique (inspi		
	La participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée (CÉSTQ)	
	Le projet de l'IdO doit contribuer à améliorer les pratiques démocratiques, mais aussi être objet de la délibération démocratique (CÉSTQ, FAP	
	Droit à soustraire ses données: Donner aux citoyens la possibilité de soustraire leurs données lorsque possible (Seattle, Euro 2018)	
	Débattre des décisions éthiques difficiles: plutôt que de les voir comme des problèmes, l'absence de solutions évidentes et protocoles de gou	
Respecter la vie privée		
Protéger et respecter la vie privée des citoyens		
	Détermination des fins de la collecte: Informer le sujet des informations collectées et de la finalité de la collecte avant ou lors de la collecte (N	
	Consentement: Les informations doivent être collectées avec le consentement des individus (Normes Canada - FIPPs, OCDE, ACM)	
	Limitation de la collecte: L'organisation ne peut recueillir que les informations nécessaires aux fins déterminées et doit procéder de façon hor	
	Utilisation pour les fins annoncées: Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles a	
	Durée de vie des données: On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins	
	Qualité de données: Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont dest	
	Vie privée par défaut: Respecter la vie privée comme paramètre par défaut - automatique protégé (Ontario, VPDC)	
		Anonymisation: les renseignements personnels devraient être anonymisés par défaut avant de rendre l'information publ
		Éviter la réidentification des données: notamment en identifiant les possibles vecteurs de réidentification des données
		Favoriser les informations ouvertes anonymisées et agrégées (Lignes IdO)
		Vie privée dans un environnement de données massives: Lorsque des bases de données sont croisées, considérer les per
		Les tierces parties sous-contractées ayant accès aux données personnelles devront se soumettre à la politique de la vie p
	Vie privée dès la conception (Ontario, VPDC)	

Figure 10. Extrait du fichier Excel mettant en relief les grands principes et les principes spécifiques (voir fichier complet dans l'Annexe G)



Compilation - Principes retenus

Principe	Détails	Sous-détails	Sources							
Bien commun										
Assurer que l'IDO soit au service du bien commun et de la démocrati										
	Le projet de l'IdO doit entraîner des bénéfices pc							CÉQ		
	Le projet de l'IdO doit se fonder sur la conciliatio							CÉQ		
	Le projet de l'IdO doit être proportionnel aux ob							CÉQ (voir formulation)		
	Les coûts ne doivent pas être socialisés alors que							CÉQ		
Démocratie et participation citoyenne										
Promouvoir la participation citoyenne pour définir une vision concer								CÉQ		
	La participation et l'engagement des citoyens et							CÉQ		
	Le projet de l'IdO doit contribuer à améliorer les							CÉQ		
	Droit à soustraire ses données: Donner aux citoy				Euro 2018	Seattle				
	Débattre des décisions éthiques difficiles: plutôt									
Respecter la vie privée										ACM (
Protéger et respecter la vie privée des citoyens										
	Détermination des fins de la collecte: Informer l	Canada							Lignes IdO (s	
	Consentement: Les informations doivent être co	Canada	FIPPs		Euro 2018	Seattle				ACM
	Limitation de la collecte: L'organisation ne peut	Canada	FIPPs		Euro 1990	Seattle				ACM
	Utilisation pour les fins annoncées: Les renseign	Canada	FIPPs		Euro 1990				same	ACM
	Durée de vie des données: On ne doit conserver	Canada							Lignes IdO (formulation in	ACM
	Qualité de données: Les renseignements person	Canada	FIPPs		Euro 1990			CÉQ (à deux endroits)		ACM
	Vie privée par défaut: Respecter la vie privée cor			Ontario			Priv b Design			
		Anonymisation: les renseign							Lignes IdO	
		Éviter la réidentification des								
		Favoriser les informations o							Lignes IdO	

Figure 11. Extrait du fichier Excel mettant en relief les principes spécifiques et les sources (voir fichier complet dans l'Annexe G)

4.1 Analyse des chevauchements entre le cadre proposé et la revue de littérature

Dans une perspective d'amélioration de la liste de principes finale, il a été jugé utile d'analyser les chevauchements entre ce cadre et les résultats de la revue de littérature (Russo Garrido et al, 2017). Conséquemment, les enjeux et menaces identifiés dans la revue de littérature et non couverts (ou partiellement couverts) dans les listes/cadres consultés ont été répertoriés.

Pour rappel, les enjeux éthiques et sociaux clés identifiés dans la revue de littérature étaient : la vie privée, la fiabilité et la transparence, l'inclusion, l'indépendance des pouvoirs publics, la liberté, la transformation de la gouvernance et la transformation de la ville.

De façon générale, les enjeux documentés, ainsi que leurs menaces identifiées dans la revue de littérature (tel que présenté dans les Figures 2, 3 et 4) sont relativement bien couverts par le cadre de principes proposé. Ci-dessous ce trouve un bilan succinct des chevauchements et angles morts existants:

- Les enjeux de la transparence, l'inclusion et l'indépendance des pouvoirs publics, tels que formulés dans la revue de littérature, sont couverts dans le cadre proposée.
- Les enjeux de la vie privée et la transformation de la gouvernance, tel que formulés dans la revue de littérature, sont couverts dans le cadre proposé (sous vie privée, sécurité, bien commun), mais quelques principes seraient à ajouter pour arriver à une couverture complète (ajouts mineurs).
- L'enjeu de la liberté n'est pas couvert dans le cadre proposé, au-delà des approches de protection de la vie privée. Quelques ajouts seraient à faire (au niveau des principes généraux et spécifiques) pour arriver à une couverture complète.
- L'enjeu de la transformation de la ville n'est que partiellement couvert dans le cadre, via le principe du bien commun. Quelques ajouts seraient à faire (au niveau des principes spécifiques) pour arriver à une couverture complète.

Le tableau ci-dessous identifie des formulations préliminaires de principes proposés pour ajout dans la liste des principes finale. Ces ajouts sont présents à même l'Annexe G et au Tableau 8[17] ci-dessus.

Tableau 9: Principes complémentaires issus de la revue de littérature.

Enjeux de la liberté dans la revue de littérature
Assurer que le citoyen ne fasse pas constamment l'objet de suivi dans sa vie quotidienne et l'informer du suivi effectué
Assurer que le citoyen ait pleinement le choix de ne pas dépendre d'analyses prédictives qui orientent ses choix
Assurer que les situations dans lesquelles l'accès des citoyens soit décidé par le biais d'analyses perscriptives soient limités, documentés de façon accessible au citoyen et puissent faire l'objet de recours de la part du citoyen, dans des délais raisonnables
Enjeux de la transformation de la ville dans la revue de littérature - classés sous bien commun dans la liste de principes
Comprendre les perceptions et craintes de la population montréalaise par rapport au projet de l'IdO
Veiller à l'analyse des conséquences à long terme du projet de l'IdO sur les valeurs sociales élargies (FAPPs) et sur l'environnement, en particulier l'émission des GES occasionnées par le projet, à travers le monde
Toute décision émanant du projet de l'IdO doit être rattachée à responsabilité décisionnelle humaine
Le projet de l'IdO doit viser l'optimum social - pas seulement l'optimisation des services/processus
Les preneurs de décisions municipaux doivent être conscients des angles morts existant dans les données et projets (ex: amélioration des services) liés à l'IdO, en particulier par rapport aux populations vulnérables
Le projet de l'IdO doit contribuer à la cohésion sociale, plutôt que l'individualisation de la ville

4.2 Prochaines étapes pour faire évoluer le cadre

Bien que la liste de principes proposée soit le résultat d'un travail méticuleux visant à rassembler les meilleurs principes existants à ce jour pour aborder les enjeux éthiques et sociaux du système de l'IdO, tel que planifié pour la ville de Montréal, plusieurs étapes doivent encore être franchies afin de parfaire cette liste et surtout, pour la rendre pleinement utile. Les Secions 4.2.1 et 4.2.2 présentent des étapes ultérieures recommandées pour une amélioration continue de la liste.

4.2.1 Renforcer certains principes

Bien que la liste de principes proposée cristallise les principes pertinents trouvés dans des listes existantes, il convient de souligner que quelques principes qui s'y retrouvent sont aujourd'hui reconnus comme étant peu efficaces/à renforcer. Ces principes sont tous afférents à la vie privée, notamment :

- La détermination des fins de collecte
- Le consentement avant ou pendant la collecte
- La limitation de la collecte de données (seulement aux fins pré-déterminées)
- Considérer les dangers potentiels à la vie privée dus à des croisements de données

Tel que discuté en détail dans la revue de littérature (Russo Garrido et al, 2017), les trois premiers principes sont alignés avec les principes de gestion de la vie privée informationnelle en vigueur au cours des dernières décennies. Cependant, tous ces principes vont directement à l'encontre de plusieurs objectifs poursuivis par le système de l'IdO et/ou ne sont pas facilement praticables dans un environnement urbain où les données sont captées en continu.

[17] Dans le Tableau 8, qui ne traite que des grands principes (et non les spécifiques), le seul changement qui a été nécessaire de réaliser a été d'ajouter un principe relatif à la liberté.

La limitation de la collecte de données et la pré-détermination des fins de collecte sont porteuses d'enjeux dans un projet où il est visé de tirer parti d'un contexte de données massives où le volume de données est synonyme de potentialités et la réutilisation des données est prévu, pour stimuler l'innovation. En effet, l'IdO remet en question notre compréhension des données « en les rendant infiniment connectables, ré-utilisables, mises à jour continuellement et facilement étriquées de leur contexte de collecte » (Metcalf and Crawford, 2016)[18].

Le consentement est également difficile à transposer dans une pratique concrète, dans un environnement où les données sont captées en continu et où il est difficile de procéder au consentement individuel de tous les citoyens touchés par cette collecte de données. Finalement, bien que les dangers potentiels à la vie privée dus à des croisements de données sont reconnus comme étant un énorme enjeu, il n'est pas clair comment, dans la pratique, mettre en œuvre ce principe de manière efficace. Davantage de réflexions et de recherches sont nécessaires pour trouver comment rendre à nouveau ces principes utiles et pertinents dans la gouverne de la ville.

Il semble que pour aborder toutes ces questions, il soit nécessaire de repenser les contours mêmes de ce qui est entendu communément par la vie privée dans un espace public comme la ville. En effet, la vie privée souvent associée aux concepts de l'intimité, du « chez-soi » et des renseignements personnels. Cependant, la possibilité de capter des informations sur les individus dans des espaces publics ouvre la question à savoir si ces informations sont de nature privée ou pas et dans quels cas elles pourraient l'être.

Helen Nissenbaum avance l'idée que la vie privée est avant tout basée sur le contexte de l'échange d'information, donnant naissance à des normes propres à cet échange (Nissenbaum, 2004; Barocas et Nissenbaum, 2014). Une information peut ou pas être partagée sans violer la vie privée, selon l'interaction entre plusieurs facteurs, comme la relation entre les parties impliquées, le niveau de sensibilité des informations, ou la direction de l'échange (bi- ou unidirectionnel)[19], tel que schématisé dans la Figure ci-dessous. Loin d'être dichotomique, la vie privée dépend donc du contexte plutôt qu'à la nature même des informations communiquées. Conséquemment, Nissenbaum (2014) avance que les individus peuvent avoir un droit à la vie privée dans un espace public.

[18] À l'origine, cette citation traitait du contexte des données massives. Cependant, elle s'applique tout autant au système de l'IdO, qui fait lui-même appel aux données massives.

[19] Ceci est appelé le principe de l'intégrité contextuelle (Barocas et Nissenbaum, 2014). Par exemple, les normes informationnelles dans le contexte d'un service de santé, établissent les informations transmissibles entre les acteurs (ex : patient, médecin, personnel administratif, famille). Dans ce contexte, le patient qui donne accès à ses informations personnelles peut le faire dans le respect de sa vie privée, si celles-ci sont gérées en accord avec les normes et les attentes sociales en terme de divulgation, partage et confidentialité.

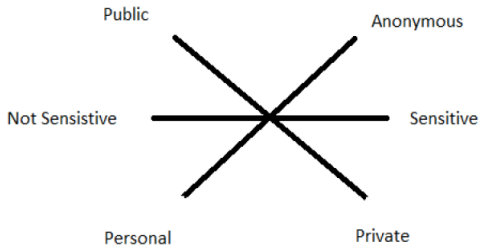


Figure 12: Certains facteurs considérés dans la vie privée contextuelle (Gaughan, 2016, 17).

Il est de l'intuition de l'équipe de recherche que ces réflexions, plaçant la vie privée dans un contexte situationnel, d'échange et non-dichotomique, peuvent ouvrir la voie vers une un réflexion susceptible de dénouer l'épineux problème du « que faire » face à certains principes de la vie privée cités à maintes reprises, mais clairement dépassés et inadéquats au contexte actuel.

4.2.2 Prochaines étapes proposées

Les prochaines étapes proposées pour faire évoluer la liste visent globalement à débattre, sélectionner, valider et renforcer les principes proposés. Elles comprennent :

- Débattre et valider des 10 principes proposés
- Débattre, reformuler, sélectionner et valider les principes spécifiques répertoriés – notamment, il sera nécessaire de statuer de quel niveau de spécificité est souhaité et s'il est préférable de prioriser quelques principes spécifiques par rapport à d'autres. Les formulations finales devront également être réfléchies, afin de viser les formulations optimales.
- Identifier les principes spécifiques manquants, entre autres en réfléchissant à ses chevauchements avec des documents de référence et à son applicabilité aux différentes étapes du système de l'IdO – une analyse approfondie des principes potentiellement manquants sera nécessaire. Tel que présenté précédemment, les principes se basent sur les listes/cadres/codes de principes existants. Conséquemment, sa couverture et ses angles morts sont tributaires des listes existantes. Il faut donc soumettre la liste de principes à une critique et analyse approfondie, afin d'en faire ressortir les points manquants.
- Renforcer les principes spécifiques faibles – tel que discuté dans la Section 4.2.1
- Étendre le dialogue sur la liste de principes au-delà de l'administration municipale – à l'instar de la municipalité de Seattle, qui a rassemblé des membres de la société civile afin de développer son cadre de principes sur la vie privée, la Ville de Montréal gagnerait à inclure des parties prenantes pour débattre et apporter leur éclairage quant au cadre proposé. Ces acteurs pourraient jouer une fonction de remise en question et contribuerait à collectiviser le projet de l'IdO.
- Identifier comment le cadre se décline en pratiques spécifiques à différentes étapes du système de l'IdO – Tel qu'illustré dans la Figure 13, il est impératif de pouvoir traduire les principes énoncés en pratiques spécifiques, applicables dans le quotidien des fonctionnaires de l'administration publique.

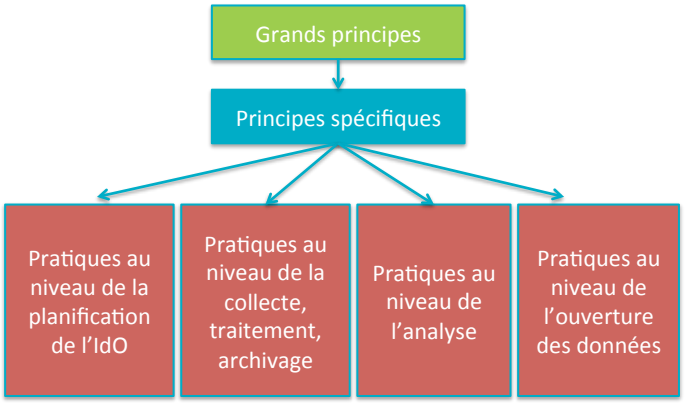


Figure 13. Déclinaison des grands principes en principes spécifiques et pratiques.

5 Conclusion

En somme, les cadres proposés dans ce rapport visent à alimenter la réflexion au sein de la Ville de Montréal sur le développement d'un (des) cadre(s) conceptuel(s) pour la gouverne éthique du système de l'IdO. Les premiers s'attèlent à la tâche d'appuyer les preneurs de décision dans la tâche d'identification des enjeux éthiques et d'acceptabilité sociale existants et émergeants. Le second s'attarde à distiller les principes généraux et spécifiques susceptibles de servir de bonne base pour bâtir une liste de principes mise de l'avant par la Ville pour l'analyse et la gestion des enjeux éthiques.

Tel que mentionné précédemment, ces éléments ne constituent pas, à eux seuls, des cadres conceptuels complets. Cependant, ils sont des jalons non négligeables vers le développement d'un cadre évolutif plus complet. À terme, ces éléments pourront porter main forte à l'implantation de pratiques optimales d'analyse, de gestion et d'intervention en matière d'enjeux éthiques et d'acceptabilité sociale en lien avec le système de l'IdO au sein de la Ville de Montréal. En effet, on ne peut faire face à l'incertitude et les transformations sociales occasionnées par l'implantation de nouvelles technologies dans la Ville qu'en se dotant d'outils pour appuyer la veille continuelle des enjeux émergeants et le développement de principes et pratiques afférentes pour contribuer à débattre des marches à suivre et des choix de société à opérer.

6 Références

ACM (2017). The 2018 ACM Code of Ethics and Professional Conduct : Draft 2. Update of the ACM Council 10/16/92. En ligne: https://ethics.acm.org/2018-code-draft-2/ Consulté le 20 décembre 2017.

Future of Life Institute (2017). ASILOMAR AI Principles. En ligne: https://futureoflife.org/ai-principles/ Consulté le 20 décembre 2017.

Cate, Fred. H. (2006) 'The Failure of Fair Information Practice Principles'. In Consumer Protection in the Age of the Information Economy. Pp.343-379.

Cavoukian, Ann (2012). Privacy by design. IEEE Technology and Society Magazine, 31:4, p-18-19.

CÉSTQ (2017). La ville intelligente au service du bien commun : Lignes directrices pour allier l'éthique au numérique dans les municipalités du Québec. Gouvernement du Québec, 112 pp.

Commissaire à l'information et à la protection de la vie privée de l'Ontario (2015). Transparency, Privacy and the Internet : Municipal Balancing Acts. Gouvernement de l'Ontario, 24 pp.

European Parliament (2016). Regulation (EU) 2016/679 of the european parliment and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data. European Union.

Forum AI Responsable (2017). Déclaration de Montréal pour un développement responsable de l'intelligence artificielle. En ligne: https://www.declarationmontreal-iaresponsable.com/la-declaration Consulté le 20 décembre 2017.

Gaughan, M (2016). Privacy in the Smart City: Implications of sensor network design, law, and policy for locational privacy. Master's thesis. Urban Studies, University of Washington.

IEEE (2017). Code of Ethics and Professional Conduct. En ligne: https://www.ieee.org/about/corporate/governance/p7-8.html Consulté le 20 décembre 2017.

IEEE (2017b). IEEE Mission and Vision. En ligne : https://www.ieee.org/about/vision_mission.html Consulté le 20 décembre 2017.

Jones, M.L. (2015). The Ironies of Automation Law : Tying Policy Knots with Fair Automation Practices Principles. Vand. J. Ent. & Tech. L., Vol. 18 pp.77-193.

Kitchin, R (2016). Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Metcalf, J. and Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. Big Data & Society, January-June, pp.1-14.

Ministère de la Justice (2017). 'Principes énoncés dans la norme nationale du Canada intitule Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96' dans CANADA, Loi sur la protection des renseignements personnels et les documents électroniques: L.C. 2000, ch. 5, à jour au 3 juillet 2017 [Ottawa], Ministère de la Justice, 2017, annexe 1, article 5.

New York City (2017). NYC Guidelines for the Internet of Things. En ligne : https://iot.cityofnewyork.us Consulté le 20 décembre 2017.

New York City Innovation & Technologies Workgroup (sans date). NYC Guidelines for the Internet of Things. The NYS Forum.

OCDE (2013). Lignes directrices régissant la protection de la vie privée et les flux tranfrontalières de données de caractère personnel. En ligne : http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm Consulté le 20 décembre 2017.

Richards, N. M. and King, J. H. (2014). Big Data Ethics. Wake Forest Law Review 49: 393-432.

Riek L. et Hartzog, W. and Howard D. et al (2014) The Emerging Policy and Ethics of Human Robot Interaction. Proceedings of the Tenth Annual ACM/IEEE International Conference on human-robot interaction extended abstracts, 02 March 2015, pp.247-248

Rosenberg, Scott (2017). 'Why AI Is Still Waiting For Its Ethics Transplant' in Wired. Novembre 2017. En ligne:https://www.wired.com/story/why-ai-is-still-waiting-for-its-ethics-transplant/?mbid=email_onsiteshare Consulté le 20 décembre 2017.

Russo Garrido, S., Allard, M.C., Merveille, N. et al (2017). Rapport final #1 pour le Lot 5 du projet Élaboration des standards pour l'IdO -- Revue de littérature : Enjeux éthiques et acceptabilité sociale de l'IdO dans la ville intelligente. Rapport livré à Jean-Martin Thibault en novembre 2017.

Zook, M., Barocas, S. boyd, d. Crawford, K., Keller E, Gangadharan SP et al e1005399 (2017). Ten simple rules for responsible big data research. Editorial. ." PLOS Computational Biology 13(3).

Annexe A:
Liste intégrale des principes extraits pour analyse

Cette Annexe est disponible ci-dessous et dans le deuxième onglet du Fichier Excel “Compilation finale principes 10 12 2017 »

Annexe B:
Valeurs et principes de la Ville intelligente au service du bien commun (CÉSTQ, 2017)

B. Les valeurs et principes de la Commission d'éthique sciences et technologie du Québec, dans son avis sur la ville intelligente (2017)

Démocratie

- ☐ L'autorité publique doit répondre à des exigences de légitimité démocratique et faire usage de sa souveraineté sur son territoire en conséquence. Les individus ne sont pas que des consommateurs de services publics, mais aussi, et surtout, des acteurs politiques.
- ☐ L'autorité publique est soumise à des normes éthiques de responsabilisation, de confiance, de transparence, de poursuite du bien commun et d'inclusion.
- ☐ L'utilisation d'un moyen numérique comme soutien aux dimensions participative, délibérative, représentative ou décisionnelle doit assurer l'inclusion du plus grand nombre de citoyens et de points de vue possible, et non une surreprésentation de la portion la plus « branchée » de la population.
- ☐ Le numérique doit être non seulement un moyen d'améliorer les pratiques démocratiques, mais aussi un objet de la délibération démocratique.
- ☐ « [L]a participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée du développement et assurer sa durabilité sur les plans environnemental, social et économique ».

↳ *– Loi sur le développement durable, art. 6 e) « participation et engagement »*

Subsidiarité

« [L]es pouvoirs et les responsabilités doivent être délégués au niveau approprié d'autorité. Une répartition adéquate des lieux de décision doit être recherchée, en ayant le souci de les rapprocher le plus possible des citoyens et des communautés concernés ».

↳ *– Loi sur le développement durable, art. 6 g) « subsidiarité »*

Responsabilité

- ☐ Un préjudice indu, ou un risque indu de préjudice, ne doit pas être infligé à autrui, que ce soit intentionnellement ou non (**non-malfaisance**).
- ☐ Des mesures suffisantes et raisonnables doivent être prises afin de réduire le plus possible les préjudices et les risques de causer des préjudices (**diligence raisonnable**).
- ☐ Des mises en garde sur les risques encourus par l'usage des données ainsi que des métadonnées de qualité doivent être publiées dans une forme compréhensible et facilement accessible pour favoriser un usage approprié des données, proportionnel à leur nature et à leur qualité (voir ci-dessous le **principe de proportionnalité** s'y rapportant).
- ☐ « [E]n présence d'un risque connu, des actions de prévention, d'atténuation et de correction doivent être mises en place, en priorité à la source ».

↳ *– Loi sur le développement durable, art. 6 i) « prévention »*

Proportionnalité des moyens par rapport aux fins

- ☐ Les moyens mis en œuvre doivent être rationnellement liés et proportionnels aux fins qui sont poursuivies.
- ☐ Dès que des données sensibles entrent en jeu, les moyens doivent se limiter à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, et le moyen qui porte le moins atteinte aux droits et libertés doit être privilégié.
- ☐ Les applications relatives à la sécurité doivent toujours s'accompagner d'une réflexion sur les causes des menaces et sur l'adéquation entre les risques perçus (par les citoyens, par les décideurs politiques) et les risques réels, afin de ne pas reproduire ou renforcer des relations de pouvoir ou des inégalités sociales par le profilage que permettent les technologies numériques.

Proportionnalité de la nature et de la qualité des données par rapport à leurs usages

- ☐ Les moyens mis en œuvre, dont les applications technologiques, doivent être nourris par des données qui sont pertinentes, fiables, complètes et adaptées à l'usage que l'on projette d'en faire.
- ☐ La qualité interne des données – leurs caractéristiques internes et généalogiques, telles que leur actualité, leur exhaustivité et leur source – doit être définie pour déterminer si elles sont aptes à satisfaire les besoins pour lesquels elles sont constituées.

Bien commun

- ☐ La sphère publique est autonome par rapport aux intérêts privés (**autonomie**).
- ☐ Dans les décisions publiques, l'intérêt public prime sur les intérêts privés (**primauté**).
- ☐ La décision publique se fonde sur la conciliation des valeurs, des perspectives et des intérêts pluriels présents dans la société civile et sur la recherche du consensus (**inclusion**).
- ☐ Les projets de ville intelligente doivent entraîner des bénéfices pour la collectivité (**utilité**).
- ☐ Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (**équité**).

Équité

- ☐ Le traitement accordé aux différentes parties doit être juste et impartial, et les disparités en la matière doivent être rigoureusement justifiées en des termes acceptables par tous.
- ☐ Les bénéfices et les inconvénients (dont les coûts) liés à l'innovation doivent être distribués équitablement entre les territoires, ce qui n'implique pas d'aplanir des disparités normales et légitimes telles que celles liées à la densité de population ou à l'accès aux ressources, ou découlant de l'application de principes comme la maximisation des bénéfices collectifs (**justice spatiale**).
- ☐ Une attention particulière doit être portée aux conséquences des projets de ville intelligente sur la fracture numérique, c'est-à-dire sur les inégalités d'accès et d'utilisation liées au numérique et à ses bénéfices qui résultent de diverses conditions matérielles, sociales et cognitives et qui touchent différentes populations, qu'elles soient composées de personnes âgées, précaires, marginalisées, peu scolarisées ou en situation de handicap (**inclusion numérique**).
- ☐ « [L]es actions de développement doivent être entreprises dans un souci d'équité intra et intergénérationnelle ainsi que d'éthique et de solidarité sociales ».

  ↳ *– Loi sur le développement durable, art. 6 b) « équité et solidarité sociales »*

Protection de la vie privée, de la confidentialité et de la sécurité des données sensibles

☐ Le principe de proportionnalité des moyens par rapport aux fins doit être appliqué.

La Loi canadienne sur la protection des renseignements personnels et les documents électroniques énonce une série de principes relatifs à l'équité dans le traitement de l'information. De même, l'OCDE publie les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, qui contiennent aussi des principes fondamentaux. Enfin, le Commissaire à l'information et à la protection de la vie privée de l'Ontario a proposé, dans les années 1990, sept principes de la protection intégrée de la vie privée (PIVP), qui forment un cadre reconnu dans le monde entier en la matière.

La Commission considère que ces ensembles de principes peuvent servir de cadre de référence pour la réflexion sur la modernisation du cadre légal. Les municipalités peuvent aussi se référer à ces principes afin de prévenir les risques juridiques liés à la protection de la vie privée. Ces principes demeurent pertinents, même à la suite des développements technologiques qui posent des défis dans le cadre légal actuel. Leur application doit cependant être repensée au regard des nouvelles situations. Voir l'annexe 4

Annexe C:
Les Lignes directrices pour les villes intelligentes et équitables

C. Les Lignes directrices pour les villes intelligentes et équitables.

Lignes directrices lancées par la ville de New York, originalement sous le le nom de « NYC Guidelines for the Internet of Things » puis ensuite Lignes directrices pour les villes intelligentes et équitables. Ces lignes directrices ont été lancées en 2016 et depuis, plus de 30 villes les ont signées, dont la ville de Paris.

Principle 1: Privacy and Transparency

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

1.1: The City should make processes and policies related to IoT and IoT-related data publicly available in an up-to-date, clear and comprehensive manner. IoT principles, guidelines, operational policies and responsibilities should be transparent and made public via a City government website.

1.2: IoT data should only be collected, transmitted, processed and used for specified, explicit and legitimate purposes. The purpose of data collection (e.g., a use case such as monitoring air quality), what data is collected (e.g., particulates in the air) and how data is being collected (e.g., pollution sensor on a light pole) should be transparent and made public via a City government website or other public notice.

1.3: Data and information collected by IoT devices should be classified and treated accordingly, per the City of New York's Data Classification Policy, as Public, Sensitive, Private or Confidential. All personally identifiable information (PII) should be classified at a minimum as private. All data that is classified as being confidential, or personally identifiable, should be protected from unauthorized use and disclosure (link to New York City Data Classification Policy).

1.4: PII should by default be anonymized before being shared in any way that could make the information publicly searchable or discoverable. Any copies and reproductions must have the same or higher level of classification as the original. Any combinations of data should be reclassified according to the City's Data Classification Policy. (Link to New York City Data Encryption Policy).

1.5: PII data types should have a clearly associated retention policy and disposal procedure. Sensitive, private or confidential data should be kept for no longer than is operationally necessary or required for the specified, explicit and legitimate purposes. (Link to New York City Digital Media Re-use and Disposal Policy).

1.6: Before any sensitive, private, or confidential data is shared outside the originating City agency, the agency should ensure that the need cannot be met by using anonymized or aggregated data and that the appropriate protections are in place to preserve the confidentiality of the data.

1.7: All public data sets are subject to the NYC Open Data Law and as such should be freely accessible via the City's Open Data portal.

Principle 2: Data Management

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

2.1: IoT systems (e.g. how data is collected, analyzed and used) should be designed with the use case in mind (e.g. predicting demand for trash pick-up based on data on trash volume, weather and events) to maximize the benefits that can be derived data collection (e.g. routing garbage trucks more efficiently). Where useful, relevant business and historical data from the City or its partners should be made available and utilized by applications.

2.2: The desired measurement from any IoT system (e.g. pedestrian counts) should be collected and categorized as efficiently as possible, using as few steps and/or manipulations as necessary.

2.3: IoT data should be collected and stored according to open standards, contain relevant contextual metadata, be exposed through open, standards-based application program interfaces (APIs), and be provided with software development kits (SDKs) where applicable so it can be easily shared or combined with other data sets.

2.4: IoT data should be archived in a federated way and made accessible throughout the City through a central portal (e.g. the City's open data portal) or a catalogue of documented open APIs unless restricted by existing laws or regulations and/or doing so would compromise privacy or public safety. Data from other systems not operated by the City, such as from a private sector partner or from crowdsourcing, that could provide public benefit can also be provided in this form with the source documented accordingly.

2.5: The City recognizes the use of distinct and sometimes conflicting non-proprietary international, national, or industry standards for data and technology interfaces. In cases where standards conflict, the one that most closely aligns to the use case will be selected.

2.6: Each IoT device data set (e.g. temperature) should be validated and verified (e.g. through redundancy in data collection and/or historical data) and the resulting master copy clearly labeled before it is used, aggregated and/or released. Data should be versioned so that any updated data can be distinguished from the original and/or master copy. The retention and disposal policies for the master copy should be explicitly defined.

2.7: IoT data should be both audited and continuously monitored for accuracy and validity. This process should be automated where possible.

2.8: All data sets (e.g. 311 service requests) should be checked for geographic, social or system-driven bias (e.g. geographic differences in civic engagement) and other quality problems. Any biasing factors should be recorded and provided with the data set and corrected where possible.

Principle 3: Infrastructure

IoT devices, networks and infrastructure shall be deployed, used, maintained and disposed of in an efficient, responsible and secure manner to maximize public benefit.

3.1: To support citywide coordination of IoT deployments, City agencies should maintain an inventory of IoT devices that they deploy using a standardized format. City agencies should also maintain an inventory of the public or private assets on which devices are installed and the networks used by these IoT devices including details on the network type (e.g. LTE), security protocol (e.g. WPA), location, service level agreements, and contact information for the network and system operator.

3.2: The City should accumulate and publish, via a City government website, public information on IoT systems including but not limited to examples of deployed IoT devices (e.g. air quality sensors) and the different types of public assets (e.g. light poles) on which they are deployed.

3.3: The City should make public, via a City government website, a standardized protocol, including points of contact, for requesting access to, and approving use of, City assets for IoT deployments. Where appropriate, the City will detail restrictions on particular types of public assets and/or siting restrictions (e.g. rules for landmark or historic districts).

3.4: IoT deployments shall, where possible, leverage or repurpose existing conduit and public assets, maximize energy efficiency, and adhere to sustainable device disposal procedures.

3.5: The City should leverage existing wireless and fixed networks where possible and appropriate. Networks for IoT deployments should be selected to best support the specific use case. This should include but is not limited to ensuring appropriate security protocols, bandwidth, pricing models, and service level agreements (SLAs).

3.6: All IoT devices and network equipment installed by the City, on the City's behalf, or on City property should have clear site license agreements and established terms of service governing who is responsible for ongoing operations, maintenance, and the secure disposal of equipment. IoT devices and network equipment should be labeled clearly with the name and contact information for the responsible party.

3.7: Public assets should be instrumented in an orderly manner that minimizes clutter and allows for ease of access for replacement, repair and addition of new equipment or devices. If new conduit is being installed using public assets (e.g. to access rooftop of public buildings) or using public right-of-way (e.g. in City streets), location details must be filed with the responsible agency and use of the conduit should not be restricted to one party.

3.8: IoT systems should be designed to maximize resiliency in the event of a natural disaster (e.g. severe flooding) or other emergencies (e.g. electrical outages). Critical systems should have established emergency response plans to ensure the appropriate continuity of service.

Principle 4: Security

IoT systems should be designed and operated with security in mind to protect of the public, ensure the integrity of services, and be resilient to attacks.

4.1: IoT systems should be designed with an explicit focus on minimizing security risks (e.g. unauthorized operation or hacking, system faults, tampering, and environmental risks), limiting the potential impact from a security breach (e.g. the release of personally identifiable information), and ensuring that any compromises can be quickly detected and managed.

4.2: IoT systems should utilize established security frameworks, where possible, and ensure communication between components is tightly constrained.

4.3: Identity and access management controls should be in place to ensure that the right people have access to systems, networks, and data at the right time. Users with access to IoT systems should be identified and authenticated. Identification should be to the individual and not to the role.

4.4: All data should be protected in transit and at rest, and systems should be secured against unauthorized access or operation. Data storage mechanisms must not be easily removed from devices and systems must not have vulnerable external interfaces (e.g. unsecured USB ports).

4.5: All partners utilizing public assets and/or networks for IoT deployments should adhere to the principles and guidelines set by the City. The City has the right to restrict or revoke access to assets, devices, and public networks to protect the public interest and public safety.

4.6: The City and its partners should engage in both audit-based and continuous monitoring to ensure that systems are working and that devices have not been compromised.

4.7: Responsibilities related to security monitoring and the protection of IoT systems should be clearly defined. In the event of a breach, public and private sector entities will be required to comply with the City's breach disclosure and notification requirements.

Principle 5: Operations and Sustainability

All IoT deployments should be structured to maximize public benefit and ensure financial, operational, and environmental sustainability.

5.1: Demonstrated need, business case, and public benefit (e.g. economic, social, and environmental outcomes) should be required prior to deployment of any new IoT devices or solutions. In addition, proof of concept should be required prior to citywide deployments.

5.2: Prior to deployment, the City and its partners shall identify all stakeholder and user groups (e.g. community residents and city employees) that will be impacted by the IoT solution and establish feedback mechanisms and methods of engagement for these groups. Before and during deployment, the City and its partners should also check for and address biases in the IoT solution (e.g. information asymmetries) that may result in unintended consequences (e.g. inequitable service delivery).

5.3: The City shall prioritize access to its assets and public networks for IoT device deployments that are distributed in an equitable manner and have the greatest public benefit. Public-private partnerships and business models that offset costs or generate revenue in ways aligned with greatest public benefit are encouraged but must be closely evaluated for risk.

5.4: All projects and associated contracts or agreements should outline the "who, what, where, when, why and how" of the implementation, operations, risk management, knowledge transfer, and maintenance of IoT systems. This should include clear definitions related to system and data ownership and responsibilities.

5.5: Solutions shall be designed to be flexible and responsive to evolving needs. Agreements should enable the addition of new functions and update of components over the life of the agreement at a fair and transparent cost.

5.6: Performance metrics should be maintained for solutions. Agreements should specify intended outcomes of a solution and levels of service and provide for penalties, modifications, or terminations of the agreement in the event that the solution does not perform.

5.7: The City and its partners should reuse infrastructures and components where possible, leverage citywide contracts or agreements, and develop solutions collaboratively among agencies to avoid duplicating existing solutions or functions and extract the greatest value from investments.

5.8: All components of a solution should be implemented in a modular manner, prioritizing open standards where possible, to ensure interoperability and prevent dependency on a single vendor.

Annexe D:
Les principes pour l'IA bénéfique de ASILOMAR

D. Les principes de l'IA bénéfique de ASILOMAR

Research Issues

1) **Research Goal:** The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.

2) **Research Funding:** Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:

- How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?
- How can we grow our prosperity through automation while maintaining people's resources and purpose?
- How can we update our legal systems to be more fair and efficient, to keep pace with AI, and to manage the risks associated with AI?
- What set of values should AI be aligned with, and what legal and ethical status should it have?

3) **Science-Policy Link:** There should be constructive and healthy exchange between AI researchers and policy-makers.

4) **Research Culture:** A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.

5) **Race Avoidance:** Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.

Ethics and Values

6) **Safety:** AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.

7) **Failure Transparency:** If an AI system causes harm, it should be possible to ascertain why.

8) **Judicial Transparency:** Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.

9) **Responsibility:** Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.

10) **Value Alignment:** Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.

11) **Human Values:** AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.

12) **Personal Privacy:** People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.

13) **Liberty and Privacy:** The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.

14) **Shared Benefit:** AI technologies should benefit and empower as many people as possible.

15) **Shared Prosperity:** The economic prosperity created by AI should be shared broadly, to benefit all of humanity.

16) **Human Control:** Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.

17) **Non-subversion:** The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.

18) **AI Arms Race:** An arms race in lethal autonomous weapons should be avoided.

Longer-term Issues

19) **Capability Caution:** There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.

20) **Importance:** Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.

21) **Risks:** Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.

22) **Recursive Self-Improvement:** AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.

23) **Common Good:** Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

Annexe E:
Déclaration de Montréal

E. La déclaration de Montréal

PRÉAMBULE

Qu'elle soit naturelle ou artificielle, l'intelligence n'a pas de valeur en soi. L'intelligence d'un individu ne nous dit rien de sa valeur morale; c'est aussi le cas pour toute autre entité intelligente. L'intelligence peut néanmoins avoir une valeur instrumentale: c'est un outil qui peut nous éloigner ou nous rapprocher d'un objectif que nous valorisons. Ainsi, l'intelligence artificielle (IA) peut créer de nouveaux risques et exacerber les inégalités économiques et sociales. Mais elle peut aussi contribuer au bien-être, à la liberté ou à la justice.

D'un point de vue éthique, le développement de l'IA pose des défis inédits. Pour la première fois dans l'histoire, nous avons la possibilité de créer des agents non humains, autonomes et intelligents, qui n'ont pas besoin de leurs concepteurs pour accomplir des tâches que l'on croyait réservées à l'esprit humain. Ces machines intelligentes ne se contentent pas de mieux calculer que les êtres humains, elles cherchent, traitent et diffusent des informations. Elles interagissent avec des êtres sensibles, humains ou non humains. Bientôt, elles pourront même leur tenir compagnie, comme un parent ou un ami.

Ces agents artificiels vont donc être amenés à influencer directement nos vies. À long terme, on pourrait créer des « machines éthiques », c'est-à-dire capables de prendre des décisions en se conformant à des principes éthiques. Il faut se demander si ces développements sont responsables et souhaitables. Et il est permis d'espérer que l'IA rende nos sociétés meilleures, dans l'intérêt de tous et le respect de chacun.

Les principes et les recommandations que nous vous invitons à élaborer collectivement sont des orientations éthiques pour le développement de l'intelligence artificielle. Pour cette première phase de la déclaration, nous avons identifié sept valeurs: bien-être, autonomie, justice, vie privée, connaissance, démocratie et responsabilité. Pour chacune d'entre elles, vous trouverez une série de questions qui visent à explorer sa relation avec le développement de l'IA. Nous proposons ensuite un principe général, qui ne répond toutefois pas directement aux questions soulevées.

VALEURS, QUESTIONS ET PRINCIPES

Bien-être

Comment l'IA peut-elle contribuer au bien-être ?

Est-il acceptable qu'une arme autonome puisse tuer un être humain ? Un animal?

Est-il acceptable qu'une IA contrôle un abattoir ?

Devrait-on confier la gestion d'un lac, d'une forêt ou de l'atmosphère terrestre à une IA?

Devrait-on développer des IA capables de ressentir du bien-être ?

Principe proposé:

Le développement de l'IA devrait ultimement viser le bien-être de tous les êtres sentients.

Autonomie

Comment l'IA peut-elle contribuer à l'autonomie des êtres humains?

Faut-il lutter contre le phénomène de capture de l'attention dont s'accompagnent les avancées de l'IA ?

Faut-il s'inquiéter de ce que des humains préfèrent la compagnie des IA à celle d'autres humains ou d'animaux ?

Peut-on donner son consentement éclairé face à des technologies autonomes de plus en plus complexes?

Faut-il limiter l'autonomie des systèmes informatiques intelligents? Un humain devrait-il toujours avoir la décision finale?

Principe proposé:

Le développement de l'IA devrait favoriser l'autonomie de tous les êtres humains et contrôler, de manière responsable, celle des systèmes informatiques.

Justice

Comment s'assurer que les bénéfices de l'IA soient accessibles à toutes et à tous?

Faut-il lutter contre la concentration du pouvoir et de la richesse au sein d'un petit nombre d'entreprises en IA?

Quelles sont les discriminations que l'IA pourrait créer ou exacerber ?

Le développement de l'IA devrait-il être neutre ou chercher à réduire les inégalités économiques et sociales?

Quels types de décisions de justice pourrait-on déléguer à une IA?

Principe proposé:

Le développement de l'IA devrait promouvoir la justice et viser à éliminer les discriminations, notamment celles liées au genre, à l'âge, aux capacités mentales et physiques, à l'orientation sexuelle, aux origines ethniques et sociales et aux croyances religieuses.

Vie privée

Comment l'IA peut-elle garantir le respect de la vie privée ?

Nos données personnelles nous appartiennent-elles et devrait-on avoir le droit de les effacer?

Devrait-on savoir à qui nos données personnelles sont transmises et, plus généralement, qui les utilise ?

Est-il contraire aux règles d'éthique ou d'étiquette qu'une IA réponde à votre place à vos courriels ?

Qu'est-ce qu'une IA pourrait faire en votre nom?

Principe proposé:

Le développement de l'IA devrait offrir des garanties sur le respect de la vie privée et permettre aux personnes qui l'utilisent d'accéder à leurs données personnelles ainsi qu'aux types d'informations que mobilise un algorithme.

Connaissance

Le développement de l'IA fait-il courir un risque à la pensée critique?

Comment minimiser la circulation de fausses nouvelles ou d'informations mensongères?

Les résultats des recherches (positifs ou négatifs) en IA doivent-ils être disponibles et accessibles?

Est-il acceptable de ne pas être informé que des conseils médicaux ou légaux sont donnés par un *chatbot*?

En quel sens les algorithmes devraient-ils être transparents quant à leur processus de décision?

Principe proposé:

Le développement de l'IA devrait promouvoir la pensée critique et nous prémunir contre la propagande et la manipulation.

Démocratie

Faut-il contrôler institutionnellement la recherche et les applications de l'IA?

Dans quels domaines est-ce le plus pertinent?

Qui devrait décider - et selon quelles modalités - des normes et valeurs morales déterminant ce contrôle ?

Qui devrait choisir les « réglages moraux » des voitures autonomes ?

Faudrait-il développer un ou des labels « éthiques » pour les IA, les site web ou les entreprises qui respectent certains standards ?

Principe proposé:

Le développement de l'IA devrait favoriser la participation éclairée à la vie publique, la coopération et le débat démocratique.

Responsabilité

Qui sont les acteurs responsables des conséquences du développement de l'IA?

Comment définir un développement progressiste ou conservateur de l'IA ?

Comment réagir devant les conséquences prévisibles sur le marché du travail?

Est-il acceptable de confier une personne vulnérable aux bons soins d'une IA ? (par exemple, avec un « robot-nanny »)

Un agent artificiel comme Tay, le *chatbot* « raciste » de Microsoft, peut-il être moralement blâmable et responsable?

Principe proposé:

Les différents acteurs du développement de l'IA devraient assumer leur responsabilité en œuvrant contre les risques de ces innovations technologiques.

DÉFINITIONS

Êtres sentients

Ce sont des êtres capables d'éprouver du plaisir, de la douleur, des émotions et, plus généralement de ressentir. Dans l'état actuel des connaissances scientifiques, on peut dire que l'ensemble des vertébrés et certains invertébrés comme les poulpes sont des êtres sentients. En biologie, le développement de la sentience peut s'expliquer par la théorie de l'évolution.

Éthique (ou morale)

C'est la discipline qui réfléchit à la bonne manière d'agir, individuellement ou collectivement, en cherchant à adopter un point de vue impartial. Elle s'appuie sur des normes et des valeurs morales.

Valeurs morales

Les valeurs morales sont relatives au bien et au mal: elle permettent, par exemple, de qualifier une action comme juste ou injuste, honnêtes ou malhonnêtes, louable ou blâmable.

Valeurs épistémiques

Les valeurs épistémiques sont relatives à la connaissance: elle permettent, par exemple, de qualifier un argument comme bon ou mauvais, claire ou fumeux, pertinent ou futile.

Valeur intrinsèque

Une valeur est dite intrinsèque lorsqu'elle est une justification ultime, lorsqu'on peut la rechercher pour elle-même. Par exemple, le bien-être, l'autonomie ou la justice peuvent recherché pour eux-mêmes: ils ont donc une valeur intrinsèque.

Valeur instrumentale

Une valeur est dite instrumentale lorsqu'elle est au service d'autre chose, lorsqu'elle permet de promouvoir une valeur intrinsèque, par exemple. Ainsi l'argent ou l'intelligence sont des valeurs instrumentales qui peuvent être mise au service du bien-être, de l'autonomie ou de la justice.

Utopie

C'est un monde possible où s'incarne un ensemble de valeurs positives. Ainsi, on peut dire qu'une société où l'IA aurait libérée les gens de tous les travaux pénibles tandis qu'ils prendraient soins les uns des autres tout en développant leur potentiel personnel, est une société utopique.

Annexe F:
Code d'éthique ACM (2018)

Cette Annexe est en anglais.

F. 2018 ACM Code of Ethics and Professional Conduct: Draft 2

Draft 2 was developed by The Code 2018 Task Force.

(It is based on the 2018 ACM Code of Ethics and Professional Conduct: Draft 1)

Preamble

The ACM Code of Ethics and Professional Conduct ("the Code") identifies key elements of ethical conduct in computing.

The Code is designed to support all computing professionals, which is taken to mean current or aspiring computing practitioners as well as those who influence their professional development, and those who use technology in an impactful way. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always a primary consideration. Section 1 outlines fundamental ethical considerations. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 pertains more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to one's conduct as a computing professional. Each principle is supplemented by guidelines, which provide explanations to assist members in understanding and applying it. These extraordinary ethical responsibilities of computing professionals are derived from broadly accepted ethical principles.

The Code is not an algorithm for solving ethical problems, rather it is intended to serve as a basis for ethical decision making in the conduct of professional work. Words and phrases in a code of ethics are subject to varying interpretations, and a particular principle may seem to conflict with other principles in specific situations. Questions related to these kinds of conflicts can best be answered by thoughtful consideration of the fundamental ethical principles, understanding the public good is the paramount consideration. The entire profession benefits when the ethical decision making process is transparent to all stakeholders. In addition, it may serve as a basis for judging the merit of a formal complaint pertaining to a violation of professional ethical standards.

1. GENERAL MORAL PRINCIPLES

A computing professional should…

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect diversity. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should give consideration to whether the products of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work. When the interests of multiple groups conflict the needs of the least advantaged should be given increased attention and priority.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should be alert to, and make others aware of, any potential harm to the local or global environment.

1.2 Avoid harm.

In this document, “harm” means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified death, unjustified loss of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may unexpectedly lead to harm. In such an event, those responsible are obligated to undo or mitigate the harm as much as possible. Avoiding unintentional harm begins with careful consideration of potential impacts on all those affected by decisions.

To minimize the possibility of indirectly harming others, computing professionals should follow generally accepted best practices for system design, development, and testing. Additionally, the consequences of emergent systems and data aggregation should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

At work, a computing professional has an additional obligation to report any signs of system risks that might result in serious personal or social harm. If one’s superiors do not act to curtail or mitigate such risks, it may be necessary to “blow the whistle” to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, the computing professional should thoroughly assess all relevant aspects of the incident as outlined in Principle 2.5.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. A computing professional should be fair and not make deliberately false or misleading claims and should provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and scientific misconduct are similarly violations of the Code. One who is professionally dishonest is accountable for any resulting harm.

A computing professional should be honest about his or her own qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the “weight” of a larger group of professionals. An ACM member should exercise care not to misrepresent ACM, or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and equal justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ACM policy. Sexual harassment is a form of discrimination that limits fair access to the spaces where the harassment takes place.

Inequities between different groups of people may result from the use or misuse of information and technology. Technologies should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.

The development of new ideas, inventions, and other creative and computing artifacts creates value for society, and those who expend the effort needed for this should expect to gain value from their work. Computing professionals should therefore provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, non-disclosure agreements, license agreements, or other methods of attributing credit where it is due.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary to facilitate the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works.

Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and other work put into the public domain. Computing professionals should avoid misappropriation of a commons.

1.6 Respect privacy.

"Privacy" is a multi-faceted concept and a computing professional should become conversant in its various definitions and forms.

Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Computing professionals should use personal data only for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent of the individual(s). When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in any one of those collections in isolation.

1.7 Honor confidentiality.

Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

User data observed during the normal duties of system operation and maintenance should be treated with strict confidentiality, except in cases where it is evidence for the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities, and the computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2. PROFESSIONAL RESPONSIBILITIES

A practicing computing professional should…

2.1 Strive to achieve the highest quality in both the process and products of professional work.

Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone affected either directly or indirectly by the work. High quality process includes an obligation to keep the client or employer properly informed about progress toward completing that project. Professionals should be

cognizant of the serious negative consequences that may result from poor quality and should resist any inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High quality computing depends on individuals and teams who take personal and organizational responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and awareness of the social context in which the work may be deployed. Professional competence also requires skill in reflective analysis for recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and should include independent study, conferences, seminars, and other informal or formal education. Professional organizations, including ACM, are committed to encouraging and facilitating those activities.

2.3 Know, respect, and apply existing laws pertaining to professional work.

ACM members must obey existing regional, national, and international laws unless there is a compelling ethical justification not to do so. Policies and procedures of the organizations in which one participates must also be obeyed, but compliance must be balanced with the recognition that sometimes existing laws and rules are immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.

Quality professional work in computing depends on professional reviewing and critiquing. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computing professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care should be taken to identify and mitigate potential risks in self-changing systems. Systems whose future risks are unpredictable require frequent reassessment of risk as the system develops or should not be deployed. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in Principle 1.3.

As noted in the guidance for Principle 1.2 on avoiding harm, any signs of danger from systems should be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for Principle 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Accept only those responsibilities for which you have or can obtain the necessary expertise, and honor those commitments.

A computing professional has a responsibility to evaluate every potential work assignment. If the professional's evaluation reveals that the project is infeasible, or should not be attempted for other reasons, then the professional should disclose this to the employer or client, and decline to attempt the assignment in its current form.

Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the project is appropriate to the professional's expertise. If the professional does not

currently have the expertise necessary to complete the project the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the project with the professional after time for additional training, to pursue the project with someone else who has the required expertise, or to forego the project.

The major underlying principle here is the obligation to accept personal accountability for professional work. The computing professional's ethical judgment should be the final guide in deciding whether to proceed.

2.7 Improve public understanding of computing, related technologies, and their consequences.

Computing professionals have a responsibility to share technical knowledge with the public by creating awareness and encouraging understanding of computing, including the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.

This principle derives from Principle 1.2 – "Avoid harm to others." No one should access or use another's computer system, software, or data without permission. One should have appropriate approval before using system resources, unless there is an overriding concern for the public good. To support this clause, a computing professional should take appropriate action to secure resources against unauthorized use. Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code (such as Principle 1.4).

3. PROFESSIONAL LEADERSHIP PRINCIPLES

In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders.

A computing professional acting as a leader should…

3.1 Ensure that the public good is a central concern during all professional computing work.

The needs of people—including users, other people affected directly and indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements, design, development, testing, validation, deployment, maintenance, end-of-life processes, and disposal should have the public good as an explicit criterion for quality. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of the social responsibilities of members of an organization or group.

Technical organizations and groups affect the public at large, and their leaders should accept responsibilities to society. Organizational procedures and attitudes oriented toward quality, transparency, and the welfare of society will reduce harm to members of the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation in meeting social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to design and build systems that enhance the quality of working life.

Leaders are responsible for ensuring that systems enhance, not degrade, the quality of working life. When implementing a system, leaders should consider the personal and professional development,

accessibility, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.4 Establish appropriate rules for authorized uses of an organization's computing and communication resources and of the information they contain.

Leaders should clearly define appropriate and inappropriate uses of organizational computing resources. These rules should be clearly and effectively communicated to those using their computing resources. In addition, leaders should enforce those rules, and take appropriate action when they are violated.

3.5 Articulate, apply, and support policies that protect the dignity of users and others affected by computing systems and related technologies.

Dignity is the principle that all humans are due respect. This includes the general public's right to autonomy in day-to-day decisions.

Designing or implementing systems that deliberately or inadvertently violate, or tend to enable the violation of, the dignity or autonomy of individuals or groups is ethically unacceptable. Leaders should verify that systems are designed and implemented to protect dignity.

3.6 Create opportunities for members of the organization and group to learn, respect, and be accountable for the principles, limitations, and impacts of systems.

This principle complements Principle 2.7 on public understanding. Educational opportunities are essential to facilitate optimal participation of all organization or group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties, including experiences that familiarize them with the consequences and limitations of particular types of systems. Professionals should know the dangers of oversimplified models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their profession.

3.7 Recognize when computer systems are becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for those systems and their users.

Organizations and groups occasionally develop systems that become an important part of the infrastructure of society. Their leaders have a responsibility to be good stewards of that commons. Part of that stewardship requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, there are likely to be changes in the ethical responsibilities of the organization. Leaders of important infrastructure services should provide due process with regard to access to these services. Continual monitoring of how society is using a product will allow the organization to remain consistent with their ethical obligations outlined in the principles of the code. Where such standards of care do not exist, there may be a duty to develop them.

4. COMPLIANCE WITH THE CODE

A computing professional should…

4.1 Uphold, promote, and respect the principles of the Code.

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles expressed in the Code. Each ACM member should encourage and support adherence by all computing professionals. Computing professionals who recognize breaches of the Code should take whatever actions are within their power to resolve the ethical issues they recognize.

4.2 Treat violations of the Code as inconsistent with membership in ACM.

If an ACM member does not follow the Code, membership in ACM may be terminated.

Annexe G :
Liste de grands principes et de principes spécifiques

Cette Annexe est en partiellement présentée ci-dessous et disponible dans le premier onglet du Fichier Excel “Compilation finale principes 10 12 2017”.

G. Liste de principes finale

Valeurs et principes	Principes spécifiques	Autres principes spécifiques
Bien commun		
Assurer que l'IDO soit au service du bien commun et de la démocratie (inspiré de CÉSTQ)		
	Le projet de l'IdO doit entraîner des bénéfices pour la collectivité (CÉSTQ) (inspiré Asilomar, FAPPs)	
	Le projet de l'IdO doit se fonder sur la conciliation des valeurs, perspectives, intérêts pluriels présents dans la société civile et sur la recherche de	
	Le projet de l'IdO doit être proportionnel aux objectifs visés (CÉSTQ)	
	Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (équité)(CÉSTQ)	
	Le projet de l'IdO doit viser l'optimum social - pas seulement l'optimisation des services/processus - FORMULATION BASÉE SUR LES ENJEUX ID. DA	
	Les preneurs de décisions municipaux doivent être conscients des angles morts existant dans les données et projets (ex: amélioration des service	
	Le projet de l'IdO doit contribuer à la cohésion sociale, plutôt que l'individualisation de la ville - FORMULATION BASÉE SUR LES ENJEUX ID. DANS F	
Démocratie et participation citoyenne		
Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique (inspiré d		
	La participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée (CÉSTQ)	
	Le projet de l'IdO doit contribuer à améliorer les pratiques démocratiques, mais aussi être objet de la délibération démocratique (CÉSTQ, FAPPs -	
	Droit à soustraire ses données: Donner aux citoyens la possibilité de soustraire leurs données lorsque possible (Seattle, Euro 2018)	
	Débattre des décisions éthiques difficiles: plutôt que de les voir comme des problèmes, l'absence de solutions évidentes et protocoles de gouver	
	Toute décision émanant du projet de l'IdO doit être rattachée à responsabilité décisionnelle humaine - FORMULATION BASÉE SUR LES ENJEUX ID.	
La vie privée		
Protéger et respecter la vie privée des citoyens		
	Détermination des fins de la collecte: Informer le sujet des informations collectées et de la finalité de la collecte avant ou lors de la collecte (Norr	
	Consentement: Les informations doivent être collectées avec le consentement des individus (Normes Canada - FIPPs, OCDE, ACM)	
	Limitation de la collecte: L'organisation ne peut recueillir que les informations nécessaires aux fins déterminées et doit procéder de façon honnêt	
	Utilisation pour les fins annoncées: Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxq	
	Durée de vie des données: On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins dé	
	Qualité de données: Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés	
	Vie privée par défaut: Respecter la vie privée comme paramètre par défaut - automatique protégé (Ontario, VPDC)	
		Anonymisation: les renseignements personnels devraient être anonymisés par défaut avant de rendre l'information publiq
		Éviter la réidentification des données: notamment en identifiant les possibles vecteurs de réidentification des données
		Favoriser les informations ouvertes anonymisées et agrégées (Lignes IdO)
		Vie privée dans un environnement de données massives: Lorsque des bases de données sont croisées, considérer les perte
		Les tierces parties sous-contractées ayant accès aux données personnelles devront se soumettre à la politique de la vie priv
	Vie privée dès la conception (Ontario, VPDC)	
	*Formulation potentiellement utile: Recognize that privacy is more than a binary value: privacy is contextual [11] and situational [12], not reduct	
Transparence		
Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation (Lignes IdO)		
	Transparence de la gestion: Transparence des politiques et pratiques concernant la gestion de l'information (Normes Canada)	
	Transparence de l'identité du maître du fichier et le siège habituel de ses activités (FIPPs)	
	Transparence sur données détenues et transférées: Informer sujets des infos détenues à son sujet et communiquées à des tiers (Normes Canada	
	Transparence sur l'utilisation des données (FIPPs)	
	Recours possible pour contester l'exactitude des renseignements avec correction possible (Normes Canada - adaptation)	
	*Formulation intéressante: La ville s'engage à être ouverte et transparente par rapport au « qui, quoi, où, pourquoi et comment » de la collecte	
Sécurité		
Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques (Lignes IdO)		
	Système sécurisé: Le système IdO devrait être conçu avec l'intention de minimiser les risques de sécurité, limiter l'impact d'une brèche de sécurit	
	Renseignements personnels sécurisés: Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à	
	Notification en cas de fuites de données (Euro 2018 - et aussi FTC (de mémoire))	
	Défaillances transparentes: Les défaillances des systèmes automatisés ne devraient pas être surprenantes, silencieuses ou irrésolubles.(FAPPs)	
	Prédictibilité : Les systèmes automatisés devraient être initialement et continuellement inventoriés pour des comportements prédictibles et impr	
	*À ajouter: les mesures dans le principe 4 "Sécurity" dans les Lignes directrices ville intelligente et équitable (Lignes IdO)	
Bonne gestion des données		
Les systèmes devraient être conçus en ayant leur utilisation en tête, pour en maximiser les bénéfices (Lignes IdO)		
	*À ajouter: les mesures dans le principe 2 "Data management" dans les Lignes directrices ville intelligente et équitable (Lignes IdO)	
Évaluer et comprendre les conséquences		
Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeurs		
	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données (Seattle)	
	Les systèmes automatisés ne devraient pas être déployés sans une évaluation des risques pour l'humain dans la boucle (human in the loop) ou les	
	Comprendre les perceptions et craintes de la population montréalaise par rapport au projet de l'IdO - FORMULATION BASÉE SUR LES ENJEUX ID. D	
	Veiller à l'analyse des conséquences à long terme du projet de l'IdO sur les valeurs sociales élargies (FAPPs) et sur l'environnement, en particulier	
Inclusion et non discrimination		
Mettre tous les moyens en œuvre pour éviter le profilage, la discrimination et pour développer un projet inclusif (CÉSTQ)		
	Application relatives à la sécurité doivent s'accompagner d'un réflexion sur les possibilités de profilage et discrimination (...) (CÉSTQ, inspiré ACM)	
	Une attention particulière doit être portée aux conséquences des projets de ville intelligente sur la fracture numérique - les inégalités d'accès et	
	Considérer l'effet de la fracture numérique sur les données et les représentations émanant du projet de l'IdO (inspiré de CÉSTQ)	
	Diversité et discrimination : Les systèmes automatisés devraient réfléchir sur les biais et les choix durant le design et tester les impacts discriminat	
	Les bénéfices et les inconvénients liés à l'innovation doivent être distribués équitablement entre les territoires (CÉSTQ)	

Autonomie des pouvoirs publics	
Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés (CÉSTQ)	
	La sphère publique est autonome par rapport aux intérêts privés (autonomie) (CÉSTQ)
	Dans les décisions publiques, l'intérêt public prime sur les intérêts privés (primauté) (CÉSTQ)
Explicabilité des systèmes	
Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision	
	Pour toute décision individuelle automatisée l'individu a le droit de connaître la logique impliquée dans la décision (Euro 1990).
	Pour tout système IA qui provoque un tort (*harm*), il devrait être possible d'expliquer pourquoi (Asilomar)
	Les systèmes automatisés devraient être compréhensibles et supporter la connaissance situationnelle, via une transparence. (FAPPs)
	Concevoir systèmes pour qu'ils soient auditables (FAPPs)
	S'impliquer dans l'analyse des conséquences plus larges des pratiques de collecte et analyse des données (10 règles)
Liberté	
Assurer que le citoyen puisse préserver son sentiment de liberté - FORMULATION BASÉE SUR LES ENJEUX ID. DANS REVUE DE LITTÉRATURE	
	Assurer que le citoyen ne fasse pas constamment l'objet de suivi dans sa vie quotidienne et l'informer du suivi effectué - FORMULATION BASÉE SU
	Assurer que le citoyen ait pleinement le choix de ne pas dépendre d'analyses prédictives qui orientent ses choix - FORMULATION BASÉE SUR LES E
	Assurer que les situations dans lesquelles l'accès des citoyens soit décidé par le biais d'analyses perscriptives soient limités, documentés de façon