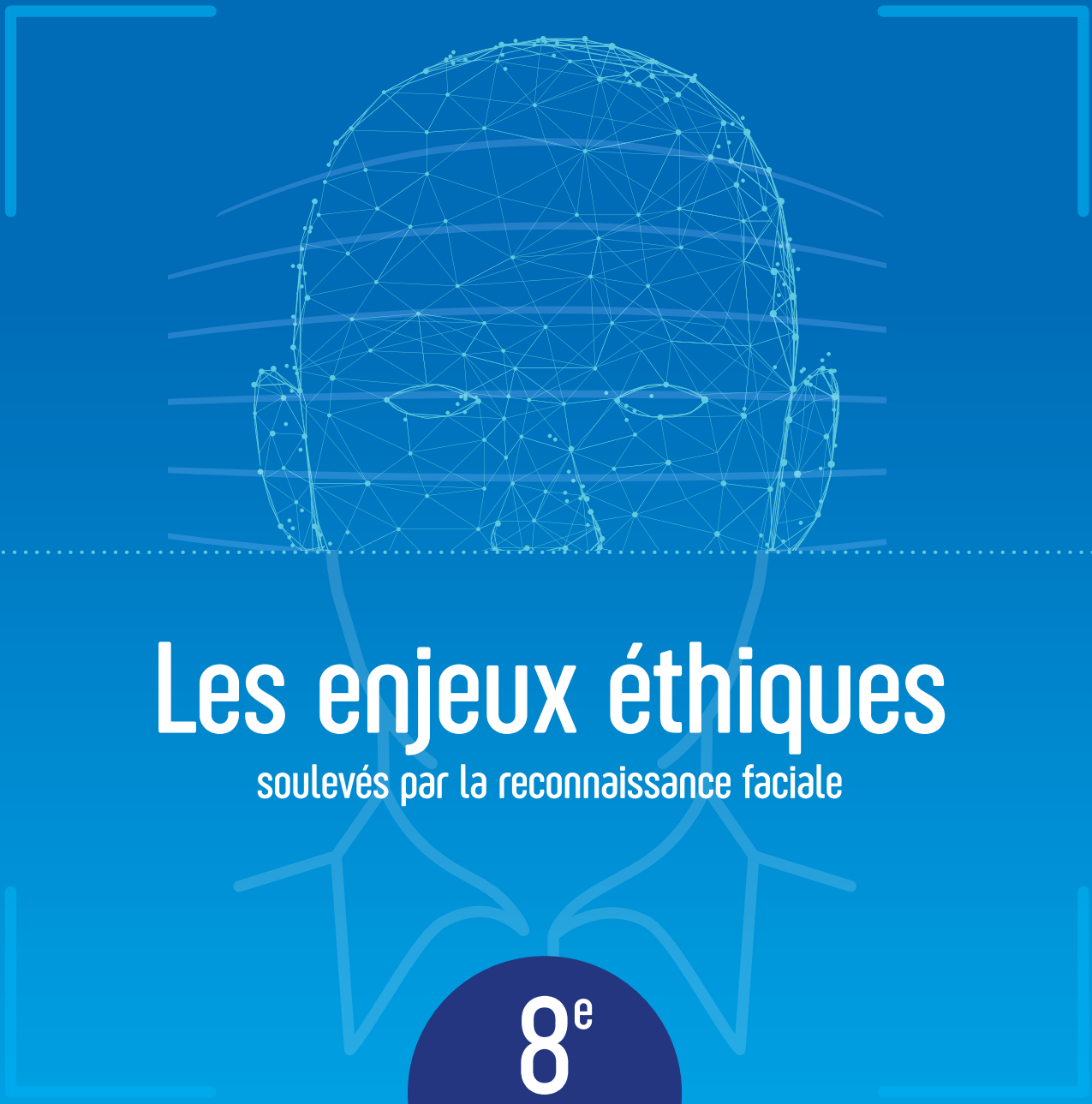


A wireframe illustration of a human face is centered in the upper half of the page. It is composed of a network of white dots connected by thin white lines. The face is framed by a light blue rectangular border with L-shaped corner brackets at each corner. A horizontal dotted line passes through the middle of the face. Below the face, there is a faint, light blue outline of a person's head and shoulders.

Les enjeux éthiques

soulevés par la reconnaissance faciale

8^e

Commission jeunesse
2020

Commission
de l'éthique
en science
et en technologie

Québec



**Commission de l'éthique
en science et en technologie (CEST)**

888, rue Saint-Jean, bureau 555

Québec (Québec) G1R 5H6

www.ethique.gouv.qc.ca

COORDINATION

Sylvain Pelletier, M.A., secrétaire général

SECRÉTARIAT

Tchonang Chimène Nandjou, adjointe administrative

RÉDACTION

Sandrine Charbonneau, B.A., stagiaire en éthique

Dominic Cliche, M.A., conseiller en éthique

David Rocheleau-Houle, Ph.D., conseiller en éthique

SOUTIEN TECHNIQUE

Révision linguistique

Magalie Allard

Graphisme, mise en page et accessibilité

Alphatek

L'avis de la CEST-Jeunesse 2020 a été déposé
à la Commission de l'éthique en science et en technologie
en avril 2020.

© Gouvernement du Québec, 2020

Image de couverture : Shutterstock

Dépôt légal : septembre 2020

Bibliothèque et archives nationales du Québec

ISBN : 978-2-550-87233-7 (PDF)

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

La CEST-Jeunesse 2020

Membres

Marie de la Sablonnière

Sciences, lettres et arts
Cégep de Sainte-Foy

Pénélope Fernandez-Busto

Sciences humaines – Affaires
internationales
Collège Jean-de-Brébeuf

Gabriel Gaudreau

Sciences humaines
Cégep de la Gaspésie et des Îles

Danaé Gilbert

Sciences de la nature
Cégep de la Gaspésie et des Îles

Louis-Charles Girard

Sciences humaines
Collège Jean-de-Brébeuf

Paa Kofi Owusu-Obimpeh

Sciences humaines
Collège Jean-de-Brébeuf

Thomas Roussel

Sciences humaines
Collège Jean-de-Brébeuf

Louis-Gabriel Roussy

Sciences humaines
Cégep de la Gaspésie et des Îles

Marie-Audrey Schembri

Sciences, lettres et arts
Cégep de Sainte-Foy

Membres et porte-parole

Fanny Caire

Sciences humaines – Affaires internationales
Collège Jean-de-Brébeuf

Karianne Cloutier

Sciences de la nature
Cégep de la Gaspésie et des Îles

Julien Guèvremont-Cornut

Soins infirmiers
Cégep André-Laurendeau

Sarah-Elizabeth Simpson

Histoire et civilisation
Cégep de Sainte-Foy

Enseignants accompagnateurs

Dave Anctil, Collège Jean-de-Brébeuf

Frédéric Bruneault, Cégep André-Laurendeau

Olivier Provencher, Cégep de la Gaspésie et des Îles

Andréane Sabourin-Laflamme, Cégep André-Laurendeau

Mathieu Saucier-Guay, Cégep de Sainte-Foy

Experts-conseil invités

Pierre-Luc Déziel, professeur à la Faculté de droit
de l'Université Laval

Sarah Gagnon-Turcotte, conseillère en stratégie
et innovation, directrice du Laboratoire de recherche
appliquée chez Nord Ouvert

Martin Gibert, chercheur au Centre de recherche en
éthique (CRÉ) et à l'Institut de valorisation des données
(IVADO)

Animatrice

Manon Lortie, professeure de philosophie,
Cégep de Jonquière

Observateurs

Dominic Cliche, conseiller en éthique à la CEST

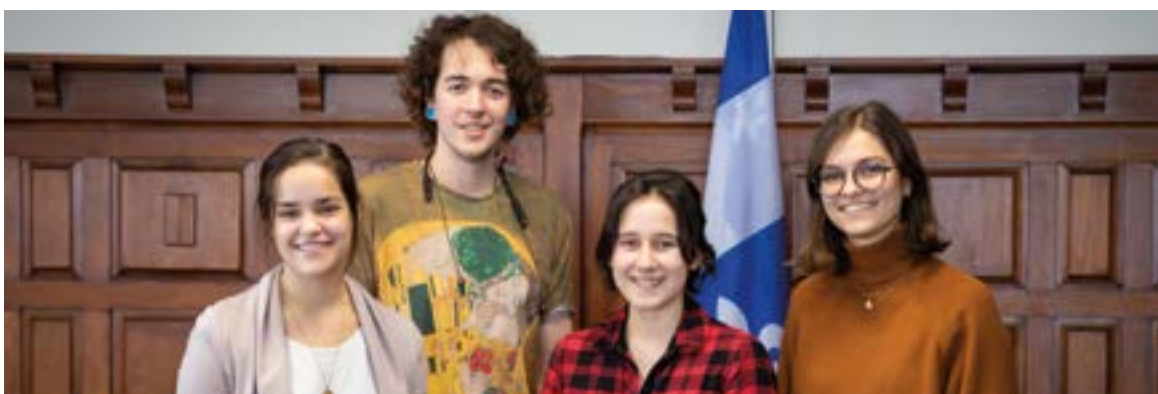
David Rocheleau-Houle, conseiller en éthique à la CEST

Table des matières

PRÉAMBULE DE LA COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE.....	5
INTRODUCTION	7
1 QU'EST-CE QUE LA RECONNAISSANCE FACIALE ?	8
• La reconnaissance faciale.....	9
• Le fonctionnement technique de la reconnaissance faciale	9
• La distinction des fonctions de la RF	10
• Les étapes du fonctionnement de la RF	10
• Les contextes d'utilisation de la RF.....	11
2 CONSIDÉRATIONS D'ORDRE ÉTHIQUE.....	16
• Efficacité, efficacité et fiabilité	17
• Égalité, équité et non-discrimination.....	18
• Transparence ou explicabilité des résultats.....	19
• Accès à l'information et développement des connaissances de la population.....	20
• Autonomie des individus.....	20
• Protection de la vie privée	21
• Sécurité.....	22
• Liberté économique des entreprises et des consommateurs.....	23
• Développement économique et prospérité	23
• Environnement et développement durable	24
• Responsabilité et imputabilité.....	24
• Indépendance des institutions publiques et bien commun.....	25
3 ANALYSE ET RECOMMANDATIONS	26
• Consentement et droit de refus	27
• Sécurité	29
• Éducation et sensibilisation	30
• Responsabilité et imputabilité	30
• Recherche	32
• Indépendance des institutions publiques	33
CONCLUSION.....	34
MÉDIAGRAPHIE.....	35
GLOSSAIRE.....	39
ANNEXE 1. Description de l'activité CEST-Jeunesse 2019-2020	41
ANNEXE 2. Programme des journées de travail de la CEST-Jeunesse 2019-2020	42



Les membres de la CEST-Jeunesse 2020 et leurs enseignants-accompagnateurs.



Les porte-paroles de la CEST-Jeunesse 2020. De gauche à droite : Karianne Cloutier, Julien Guèvremont-Cornut, Sarah-Elizabeth Simpson et Fanny Caire.



Échanges entre les membres.



Échanges entre les membres.

Recommandations

de la CEST Jeunesse

Commission
de l'éthique
en science
et en technologie

Québec



CONSENTEMENT ET DROITS DE REFUS

- 1 Que les individus puissent, dans la mesure du possible, consentir à l'utilisation de la reconnaissance faciale.
- 2 Que les individus puissent, dans la mesure du possible, refuser d'être sujet à un système de reconnaissance faciale et, ceci, sans conséquences.

RAPPEL 1

Le consentement doit être explicitement demandé lorsqu'il y a collecte de renseignements personnels sur les individus, lorsqu'il y a communication ou utilisation d'un renseignement personnel qui n'a pas été établi au préalable.



SÉCURITÉ

- 3 Que l'utilisation de la reconnaissance faciale à des fins de sécurité soit justifiée par son efficacité, sa nécessité et sa proportionnalité.

RAPPEL 2

À l'exception des conditions et des exceptions reconnues par le Code criminel canadien, la demeure est inviolable et le Gouvernement du Québec et ses organismes, ainsi que les entreprises privées, ne peuvent utiliser les technologies de la reconnaissance faciale pour s'immiscer dans celle-ci sans le consentement exprès de la personne résidente.



RESPONSABILITÉ ET IMPUTABILITÉ

- 5 Que dans les cas où il y a un préjudice possible, la reconnaissance faciale demeure un outil qui soutient la décision d'un être humain et que celui-ci, ou tout autre être humain, soit toujours impliqué.
- 6 Que le Gouvernement du Québec se dote d'une instance de surveillance et de régulation en matière d'intelligence artificielle.
- 7 Que le Gouvernement du Québec travaille à établir des normes qui seraient imposées aux développeurs et utilisateurs d'algorithmes de reconnaissance faciale, dont un processus d'homologation obligatoire pour les applications utilisées sur le territoire québécois.
- 8 Que des normes strictes soient élaborées par le Gouvernement du Québec pour encadrer l'intégration de la reconnaissance faciale dans les appareils intelligents mis en marché par le secteur privé.



RECHERCHE

- 9 Que le ministère de l'Économie et de l'Innovation et les Fonds de recherche du Québec instaurent un programme de financement de la recherche sur l'IA et la reconnaissance faciale au bénéfice de l'ensemble de la population québécoise.



INDÉPENDANCE DES INSTITUTIONS PUBLIQUES

- 10 Que le Gouvernement du Québec développe sa propre expertise interne en matière de développement en intelligence artificielle et de stockage de données, de manière à assurer son indépendance par rapport aux intérêts privés ou aux entreprises privées.



ÉDUCATION ET SENSIBILISATION

- 4 Par l'élaboration d'outils d'éducation et de sensibilisation, le Gouvernement du Québec doit informer le public, plus particulièrement les jeunes, du fonctionnement de la reconnaissance faciale, ainsi que des bénéfices et des risques associés à l'utilisation de cette technologie.

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

La Commission de l'éthique en science et en technologie (CEST) est heureuse de publier le huitième avis de sa Commission Jeunesse (CEST-Jeunesse). Cette dernière, qui portait sur l'utilisation de technologies de reconnaissance faciale, s'est déroulée de septembre 2019 à janvier 2020 grâce à la collaboration d'enseignantes et d'enseignants en philosophie au niveau collégial et de leurs étudiantes et étudiants.

Depuis 2005, la CEST réunit la CEST-Jeunesse tous les deux ans. Ce projet vise à permettre à des étudiantes et des étudiants du cégep de s'intéresser concrètement aux enjeux éthiques d'une application de la science et de la technologie et, ensuite, de vivre l'expérience du fonctionnement de la CEST et de la délibération éthique¹.

Les enjeux soulevés par les systèmes d'intelligence artificielle et, notamment, les systèmes de reconnaissance faciale, sont d'une grande actualité. En ce sens, les réflexions menées par les membres de la CEST-Jeunesse 2020 arrivent à point et constituent une contribution importante au débat public sur ces questions.

La CEST souhaite souligner la grande qualité du travail réalisé par les participantes et participants de cette édition, tant lors de la préparation que lors des journées de délibération. Elle en accueille les constats et les recommandations, qu'elle relayera aux autorités compétentes. Elle est consciente que la mise en œuvre de certaines recommandations pourrait s'avérer difficile. Cependant les objectifs derrière les recommandations, eux, ne doivent pas être perdus de vue et doivent être atteints. Autrement dit, on peut être flexible sur les moyens, mais pas sur les fins.

La CEST souhaite enfin remercier les membres de la CEST-Jeunesse et tous ceux et celles qui ont participé au succès de cet événement.

La tenue de la CEST-Jeunesse n'est possible qu'avec la collaboration d'enseignantes et d'enseignants en philosophie du réseau collégial qui acceptent de participer au projet. Pour la présente édition, une enseignante et quatre enseignants² provenant de quatre cégeps du Québec ont supervisé le travail préparatoire des étudiantes et des étudiants. Au cours de la session d'automne 2019, ils ont animé dans leurs cégeps respectifs des rencontres de réflexion et de délibération sur les enjeux éthiques soulevés par l'utilisation des technologies de reconnaissance faciale. À la suite de cela, les participantes et participants se sont réunis pour des journées de délibération sur la colline Parlementaire à Québec³. Le présent avis a été rédigé dans les mois suivant ces journées de délibération.

1 Pour plus d'informations sur l'activité, voir l'annexe 1.

2 M. Dave Anctil (Jean-de-Brébeuf), M. Frédérick Bruneault (André-Laurendeau), M. Olivier Provencher (Gaspésie et des îles), M^{me} Andréane Sabourin-Laflamme (André-Laurendeau), M. Mathieu Saucier-Guay (Sainte-Foy).

3 La composition de la CEST-Jeunesse 2020, qui comptait treize (13) membres provenant de quatre cégeps, est présentée au début de ce document. Pour plus de détails sur le programme de la fin de semaine, voir l'annexe 2.

Cette année, la CEST-Jeunesse a accueilli trois experts-conseil, M. Pierre-Luc Déziel⁴, M^{me} Sarah Gagnon-Turcotte⁵ et M. Martin Gibert⁶, qui ont chacun été présent lors d'une des journées de délibération pour répondre aux questions des étudiantes et des étudiants. La CEST tient à les remercier pour leur disponibilité et leur enthousiasme à partager leur expertise.

Elle tient enfin à remercier spécialement M^{me} Manon Lortie, une ambassadrice émérite de la CEST-Jeunesse qui en a assuré l'animation avec brio.

En donnant la parole aux jeunes et en leur permettant de jeter un regard éthique sur les enjeux qui les préoccupent, la CEST agit avec la conviction renouvelée que les avis de la CEST-Jeunesse contribuent à enrichir de façon significative le débat public. Cette année encore, par sa riche intervention dans un débat de société d'actualité, la CEST-Jeunesse démontre l'importance et l'apport du temps pris pour mener une réflexion en commun.

Le président de la Commission de l'éthique en science et en technologie,

A blue ink signature, likely of Jocelyn Maclure, consisting of stylized, flowing letters.

Jocelyn Maclure

4 M. Déziel est professeur à la Faculté de droit de l'Université Laval.

5 M^{me} Gagnon-Turcotte est conseillère en stratégie et innovation. Chargée de projet au moment de la tenue des journées de délibération, elle est maintenant directrice du Laboratoire de recherche appliquée chez Nord Ouvert.

6 M. Gibert est chercheur au Centre de recherche en éthique (CRÉ) et à l'Institut de valorisation des données (IVADO).

Introduction

Vous pouvez lui demander d’attester que vous êtes bien la personne représentée sur votre passeport, pour aller prendre votre vol plus rapidement sans devoir passer voir un agent au comptoir de l’aéroport. Elle peut déverrouiller votre téléphone. Elle peut vous reconnaître dans la foule et en avertir les autorités policières. Elle peut vous suivre au fil de vos différents achats au centre commercial. Elle peut informer votre employeur à savoir si vous êtes heureux au travail, sans que vous en soyez informé à chaque fois.

La reconnaissance faciale fait beaucoup jaser, plus souvent qu’autrement en lien avec les enjeux éthiques qu’elle soulève : protection de la vie privée, profilage, respect de la dignité des personnes, sécurité publique, etc. Les autorités publiques et les entreprises privées au Québec devraient-elles utiliser la reconnaissance faciale et, si oui, dans quelles circonstances et à quelles fins ?

La **8^e CEST-Jeunesse** s’est réunie en janvier 2020 dans l’objectif de réfléchir à cette question et de proposer des balises propres à assurer une utilisation responsable de la reconnaissance faciale. Les membres de la CEST-Jeunesse, treize (13) étudiantes et étudiants de niveau collégial, se sont demandé quels étaient les bénéfices et les risques associés aux différentes utilisations de la reconnaissance faciale, quelles valeurs étaient mises en jeu par ces utilisations, et quelles devraient être les actions prioritaires à poser pour le gouvernement du Québec. Le présent avis fait rapport des travaux de la CEST-Jeunesse 2020, de ses questionnements, de ses constats et de ses recommandations.

Dans le premier chapitre, elle répond aux questions : Qu’est-ce que la reconnaissance faciale ? Quelles en sont les principales utilisations possibles ?

Ensuite, dans le deuxième chapitre, elle répond aux questions : Quelles sont les valeurs en jeu ? Quels sont les enjeux éthiques soulevés par les utilisations de la reconnaissance faciale par les différents acteurs ?

Enfin, dans le troisième et dernier chapitre, la CEST-Jeunesse 2020 propose son analyse éthique et, surtout, formule dix (10) recommandations et deux (2) rappels à l’intention des décideurs publics.

1

**Qu'est-ce que la
reconnaissance faciale ?**

La reconnaissance faciale

La reconnaissance faciale (RF) est une technologie qui utilise des algorithmes d'intelligence artificielle (IA) pour identifier un individu sur une image ou dans une vidéo. L'utilisation classique de la RF est à des fins d'identification ou de confirmation de l'identité d'une personne avec une ou plusieurs de ses caractéristiques biologiques. C'est en ce sens que la RF fait partie de la classe plus large des systèmes biométriques, qui permettent d'identifier les individus grâce à leurs caractéristiques propres : empreinte digitale, iris de l'œil, traits du visage, etc.

La RF peut aussi être utilisée pour analyser les caractéristiques d'un individu, dont son âge, son genre, ses émotions, sans nécessairement chercher à identifier celui-ci. Dans le cadre de cet avis, la CEST-Jeunesse comprend la RF comme incluant à la fois les systèmes qui permettent d'identifier des individus que les systèmes qui permettent d'analyser ceux-ci sans nécessairement les identifier. Autrement dit, un système de RF peut être utilisé afin de procéder à l'identification, à la confirmation de l'identité ou encore à la reconnaissance des traits catégoriels (ex. l'âge ou le genre) et des états (ex. ses émotions) d'une personne.

La RF n'est pas une seule technologie, mais constitue un ensemble de technologies qui peuvent également être intégrées à d'autres technologies existantes, telles que : des caméras et capteurs de sécurité et de surveillance, des logiciels de classification de banques d'images et de vidéos, ou des algorithmes d'intelligence artificielle (IA). Divers capteurs 2D, 3D et même infrarouges captent ou traitent la présence de visages à partir de vidéos ou d'images, les comparant ensuite à une banque de données de visages et de traits, permettant la comparaison et l'établissement (ou non) de correspondances. Ces images et vidéos peuvent provenir de sources communes comme les caméras de surveillance, mais également être saisies par des téléphones mobiles (ex. pour permettre son déverrouillage), ou provenir de divers contenus déposés en ligne, comme sur les médias sociaux. Ainsi, plusieurs enjeux soulevés par la reconnaissance faciale ne sont pas propres à cette technologie, mais sont en lien avec les systèmes plus vastes qui intègrent la RF, tels que les systèmes d'intelligence artificielle.

Le fonctionnement technique de la RF

Les développements récents en matière de reconnaissance faciale ont entre autres pu voir le jour grâce aux nouvelles possibilités qu'apporte son utilisation jumelée aux technologies d'IA. Les développements récents en apprentissage machine (*machine learning*) et en particulier en apprentissage profond (*deep learning*) ont permis le développement de multiples applications en RF. Les champs qui y sont liés touchent principalement ceux de la vision par ordinateur (*computer vision*) et l'informatique affective (*affective computing*). La vision par ordinateur touche aux fonctions élémentaires de la captation, du traitement et de l'analyse d'images, permettant au système informatique de « voir ». L'informatique affective quant à elle tente d'interpréter ce qu'elle voit afin d'en reconnaître et d'en dégager les affects humains, comme les émotions.

Sur le plan des techniques d'apprentissage de l'IA, on parle de capacités accrues à repérer des corrélations à travers de larges jeux de données (comme des images ou des mots), pour ensuite établir des classifications et des prédictions très poussées concernant certains traits, caractéristiques et comportements. Les technologies d'IA ont une capacité d'apprentissage, permettant aux algorithmes de se corriger et de s'améliorer, en partie par eux-mêmes, du moins dans leur phase d'entraînement. C'est en ce sens que les algorithmes d'IA sont considérés comme étant « dynamiques ».

Le potentiel de perfectionnement apporté par l'IA ouvre de multiples possibilités, puisque les systèmes d'IA ont la possibilité de découvrir par eux-mêmes de nouvelles corrélations. Ces algorithmes deviennent de puissants outils pour authentifier et identifier les visages, ainsi que pour interpréter leurs caractéristiques. Ils sont beaucoup plus précis que les technologies de RF qui n'utilisent pas d'IA.

La distinction des fonctions de la RF

Il est possible de distinguer trois fonctions des technologies modernes de RF :

1. *La confirmation de l'identité d'une personne.* Dans ce cas, il s'agit de vérifier l'identité d'une personne. Le système de RF répond alors à la question « est-ce que la personne x est bien celle qu'elle prétend être ? ». Cette fonction permet de déterminer si une personne a bien le droit d'avoir accès à un lieu sécurisé. Dans plusieurs cas, un système de RF peut être utilisé au même titre qu'un autre système d'authentification biométrique (empreinte digitale, iris de l'œil, etc.) ou que la vérification manuelle par un agent de sécurité.
2. *L'identification d'une personne.* Dans ce cas, le système de RF cherche à répondre à la question « qui est la personne x ? ». Il ne s'agit alors pas de valider l'identité d'une personne pour que celle-ci puisse avoir accès à un lieu sécurisé, par exemple. Il pourrait plutôt s'agir de reconnaître une personne dans une foule, ou encore de trouver des photos d'une personne disponibles sur le Web à partir d'une photo connue.
3. *L'analyse des caractéristiques des visages ou d'une personne.* Dans ce cas, la RF peut être utilisée pour déterminer les caractéristiques d'une personne (âge, sexe, genre, origine ethnique, etc.), des traits de personnalité (par exemple, est-ce une personne extravertie ou introvertie ?) ou les émotions vécues par cette personne. Il ne s'agit alors pas d'authentifier ou d'identifier cette personne⁷.

Les étapes du fonctionnement de la RF

Lorsqu'il s'agit d'identifier une personne ou de confirmer son identité, le système de RF devra concevoir un gabarit à partir de l'image qu'il aura reçue. Il retiendra plusieurs points clés (plusieurs dizaines, voire plus d'une centaine selon les systèmes) qui identifient le visage. Ce gabarit sera comparé avec d'autres images afin d'estimer la correspondance avec ces dernières. Voici, sommairement, les étapes de fonctionnement d'un système de RF.

1. La détection du visage : le système détecte la présence d'un visage humain dans une image ou un vidéo, qui peut s'effectuer en temps réel ou à partir de banque de données déjà enregistrées.
2. L'analyse du visage : le système extrait les traits et peut aussi détecter les caractéristiques génériques (ex. âge, genre, couleur de peau), tout comme les caractéristiques émotionnelles du visage.

⁷ Il est également possible que le système de RF utilise plusieurs de ces fonctions en même temps.

3. L'association du visage : le système compare les données reçues avec celles de banques de données comportant d'autres visages et traits, permettant de confirmer ou d'infirmer l'identité de l'individu ou encore d'interpréter ses émotions.
4. Le système rend un résultat sur la correspondance.

Lorsqu'il s'agit uniquement d'analyser les caractéristiques des individus, sans chercher à les identifier ou à confirmer leur identité, le système pourra alors seulement accomplir les deux premières étapes.

Dans tous ces cas, il est important de retenir que la RF fonctionne de manière *probabiliste*. Le système de RF détermine la probabilité que telle personne corresponde à une image d'une base de données, que cette personne soit de sexe masculin, qu'elle exprime une émotion de joie, etc.

Il y a toujours des possibilités pour ces systèmes de commettre des erreurs (des *faux positifs*) en effectuant des correspondances erronées entre des visages ou, au contraire, en échouant à valider certaines correspondances (des *faux négatifs*). Plusieurs facteurs techniques et technologiques peuvent influencer les taux de succès et d'échec des logiciels, comme la qualité des caméras, l'éclairage et l'angle de la captation vidéo ou photo des visages, la précision des gabarits contenus dans les bases de données, ou encore la quantité et la représentativité des images contenues dans les bases de données utilisées pour comparer les visages captés.

Les contextes d'utilisation de la RF

Les technologies de reconnaissance faciale sont en croissance dans plusieurs domaines, faisant émerger une multitude de contextes d'utilisation. Du déverrouillage d'un téléphone cellulaire au passage du contrôle de sécurité à l'aéroport, passant par la détection de criminels dans les commerces et les lieux publics, les usages de la RF sont multiples.

Le secteur commercial s'intéresse lui aussi de plus en plus à la RF, avec la possibilité de pouvoir augmenter l'expérience des clients en temps réel et en amassant des données plus précises sur leurs profils et comportements d'achats. La RF représente un moyen efficace d'analyser de multiples visages dans des lieux publics ou lors d'événements où se retrouvent des foules de gens, en plus de permettre d'analyser certaines réactions des clients, ce qui est particulièrement intéressant pour le secteur commercial.

Sans prétendre offrir une liste exhaustive des contextes et des usages dans lesquels peut être utilisée la RF, voici les six catégories dans lesquelles elle est la plus souvent présente :

1. *Sécurité*. Cette catégorie englobe plusieurs usages distincts, qui sont (a) le contrôle et l'accès à des lieux, des outils et des services, (b) la prévention de crimes et le contrôle de foules et (c) la détection de violations à des règlements.
 - a. La RF permet de contrôler l'accès à certains lieux en donnant accès uniquement aux personnes autorisées d'y pénétrer (comme un bureau, une école ou une chambre d'hôtel), ou encore d'autoriser un individu à utiliser un certain outil (comme un téléphone cellulaire) ou service (comme un guichet automatique). Ces mesures ont pour but de faciliter et de sécuriser les accès et l'utilisation de ces endroits, outils et services.

- b. Pour ce qui est de la prévention de crimes, la RF peut être utilisée principalement dans des lieux publics et lors d'événements avec une foule nombreuse. La RF peut être utilisée pour détecter dans des lieux publics des individus fichés (en raison de leurs comportements et agissements suspects ou criminels), qui représenteraient un risque pour le public. Elle peut également être utilisée afin de détecter des spectateurs aux comportements agressifs lors d'un concert et, ainsi, assurer un meilleur contrôle des foules.
 - c. Dans le cas de la détection de violation à des règlements, la RF est déjà utilisée pour identifier les personnes traversant illégalement la rue lors des feux rouges en Chine. Elle a également été très utile pour retrouver des enfants disparus⁸, ou encore pour identifier des voleurs à l'étalage dans des commerces.
2. *Commerce.* La RF peut être utilisée dans le contexte commercial afin d'améliorer l'expérience client ou encore pour augmenter les profits et les connaissances des commerces sur leurs clients. Divers commerces pourraient décider d'utiliser la RF afin d'identifier le profil de leurs clients en fonction de leur identité (s'ils sont des clients réguliers), ou en fonction de certains traits (ex. leur genre ou leur âge). Avec ces informations, ils pourraient personnaliser leur expérience en magasin, par exemple en leur montrant des publicités plus ciblées de manière instantanée. De plus, la reconnaissance faciale pourrait être un moyen de récolter des données comportementales sur les clients, permettant d'avoir leurs réactions en temps réel lors de leurs activités. Par exemple, si tous les clients affichent un air d'insatisfaction devant un vêtement, ou au contraire un visage de satisfaction devant un arrangement de vitrine coloré, le commerce aurait de meilleures informations sur les préférences de leur clientèle. De plus, la RF pourrait être utilisée afin de réduire les frictions lors des achats et les besoins en main-d'œuvre en ayant, comme dans les magasins Amazon Go⁹, des commerces sans caisse. Dans ceux-ci, les clients se font identifier à leur entrée et peuvent prendre les produits qu'ils désirent, les caméras de RF et les scanners de reconnaissance de produits détecteront ce qu'ils ont pris et ils seront chargés à leur sortie, directement sur leur carte de crédit.
3. *Relation d'aide.* Grâce aux fonctions de reconnaissance d'émotion, la RF pourrait être utilisée en contexte de relation d'aide afin de détecter des individus en situation de crise. Dans des lieux publics, comme des commerces, ou même des hôpitaux, la RF permettrait aux agents de sécurité d'intervenir auprès de ces personnes en difficulté. La RF pourrait également être utilisée pour assister les personnes aveugles. Par le biais d'applications et d'outils de RF, les visages de leurs interlocuteurs pourraient être saisis et leurs traits identifiés, ce qui pourrait aider les personnes non voyantes dans leurs relations interpersonnelles.

8 L'utilisation d'un algorithme de reconnaissance faciale pour établir des correspondances entre des photos d'enfants disparus et d'enfants retrouvés mais non identifiés a permis de retrouver plusieurs milliers d'enfants en Inde. Voir NDTV (2018).

9 Harwell et Bhattarai (2018).

4. *Santé.* La RF, à l'instar de plusieurs technologies d'IA, permet déjà la détection de certaines maladies avec des taux d'identifications supérieurs à ceux des meilleurs experts du domaine, dont pour certaines maladies de peau et autres maladies aux symptômes affectant le visage. Elle pourrait même dans certains cas détecter des maladies psychiatriques comme la dépression, en cernant des détails et des réactions sur les visages qui sont parfois imperceptibles à l'œil humain. Ce domaine pourra grandement bénéficier des développements en RF, qui pourrait servir non seulement lors des diagnostics, mais également lors des suivis et des traitements. La RF pourrait être utilisée pour suivre des patients âgés, pour assurer entre autres leur protection et leur prise de médicaments.
5. *Travail.* Dans le monde du travail, la RF peut être utilisée lors du processus d'embauche et peut aussi permettre un suivi des performances et de l'état de santé des travailleurs. Chez certaines compagnies recevant de nombreuses candidatures lors d'embauches, des logiciels de RF sont utilisés afin d'analyser les traits et les émotions des candidats lorsqu'ils se filment en train de répondre à des questions de présélection. Le système de RF leur attribue un score de performance en fonction des mouvements et des expressions de leur visage. La RF pourrait aussi être utilisée afin de s'assurer de la performance et du bien-être des employés, en vérifiant par exemple leur état durant leurs journées de travail. Si un employé semble maussade, son superviseur pourrait en être informé par la RF et s'informer sur son état. La RF permet également de suivre des travailleurs sur leur lieu de travail, un entrepôt par exemple. Ici encore, la RF pourrait permettre d'associer un score de performance unique à chaque travailleur ou prévenir certaines blessures liées au travail.
6. *Divertissement.* Dans le domaine du divertissement, la RF en est encore à ses balbutiements. Plusieurs nouveaux modèles de téléphones intelligents sont équipés de caméras plus puissantes, permettant une reconnaissance du visage poussée, donnant la possibilité aux utilisateurs de créer des filtres animés sur leurs visages. Certaines applications, comme *Google Arts & Culture* et sa fonctionnalité *Art Selfie*, permettent aux utilisateurs de comparer leur visage avec une large base de données d'œuvres d'art, associant celles qui leur ressemblent le plus. Des consoles de jeux vidéo peuvent aussi être équipées d'un système de RF. La RF permet également à des comédiens de voir leurs réactions faciales reproduites au cinéma sur des personnages animés.

Fonctionnement

de la reconnaissance faciale

Commission
de l'éthique
en science
et en technologie

Québec



4 ÉTAPES

1

LA DÉTECTION DU VISAGE

Le système détecte la présence d'un visage dans une image ou un vidéo.



2

L'ANALYSE DU VISAGE

Le système extrait les traits et caractéristiques du visage.



3

L'ASSOCIATION DU VISAGE

Le système compare les données collectées avec celles de banque de données.



4

CONFIRMATION DE L'IDENTITÉ

Le système rend un résultat sur la correspondance.



**Analyse des caractéristiques des visages
ou d'une personne :**

le système accomplit uniquement les étapes **1** et **2**.



**Confirmation de l'identité d'une personne
ou identification d'une personne :**

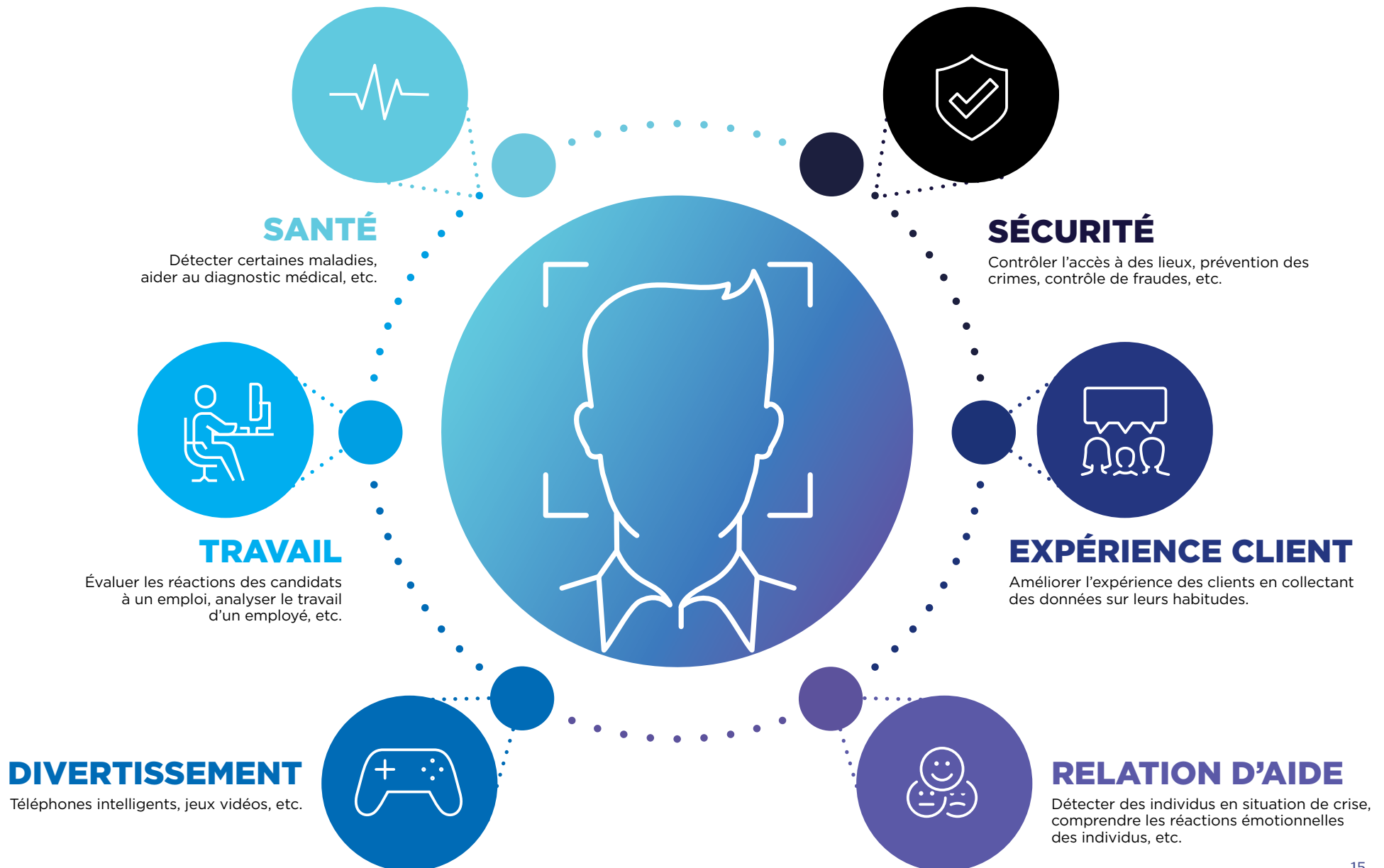
le système devra adopter les **4 étapes**.

Contexte d'utilisation

de la reconnaissance faciale

Commission
de l'éthique
en science
et en technologie

Québec



2

Considérations d'ordre éthique

Pour conduire son analyse éthique, la CEST-Jeunesse identifie tout d'abord un ensemble de valeurs qui sont mises en jeu par l'utilisation de la reconnaissance faciale, dans différentes situations. Les valeurs pertinentes à l'analyse éthique de même que leur poids relatif pourront varier d'une situation à l'autre. C'est pourquoi, en plus de présenter les valeurs, il importe de déterminer comment certaines valeurs peuvent être promues ou, à l'inverse, mises à mal dans différents contextes, selon des utilisations particulières ou selon le type de technologie en cause. Bref, il importe de déterminer quels sont les principaux enjeux éthiques.

On est en présence d'un enjeu éthique lorsqu'une valeur est mise en jeu dans une situation, ou lorsqu'on fait face à un conflit entre différentes valeurs. Dans ce dernier cas, on peut aussi parler de dilemme éthique. La CEST-Jeunesse a pu constater que l'utilisation de la reconnaissance faciale soulève un grand nombre d'enjeux. Plusieurs de ces enjeux ne sont pas spécifiques à cette technologie particulière, mais se rencontrent aussi dans d'autres contextes de surveillance des individus à des fins de sécurité, de profilage à des fins commerciales, ou de gestion des renseignements personnels. De même, plusieurs de ces enjeux reposent sur le fait que la reconnaissance faciale fait usage d'algorithmes d'intelligence artificielle; ces enjeux concernent donc d'abord l'intelligence artificielle plutôt que la reconnaissance faciale. Enfin, d'autres enjeux touchent au rôle des pouvoirs publics dans le développement et l'encadrement de la reconnaissance faciale, ainsi que des interactions entre les secteurs public et privé. Dans chacun de ces cas, les caractéristiques de la reconnaissance faciale et les différents usages qui peuvent en être faits viennent accroître des risques ou accentuer des enjeux.

Efficacité, efficacité et fiabilité

Le recours à la reconnaissance faciale est souvent justifié sur la base des gains d'efficacité ou d'efficience qu'elle permettrait de réaliser. L'efficacité est le rapport entre les résultats obtenus et les objectifs fixés. L'efficience, de son côté, est le rapport entre les résultats obtenus et les ressources utilisées pour les atteindre. Ainsi, une technologie est efficace si elle permet de réaliser entièrement l'objectif pour lequel elle est déployée; elle est efficiente si elle permet d'atteindre cet objectif en faisant une utilisation optimale des ressources disponibles. Cette valeur peut être interprétée du point de vue environnemental pour étayer des principes de développement dit durable ou soutenable, tels que la réduction des déchets et la maximisation des matières réutilisées ou recyclées dans le cycle de vie de la technologie, l'efficacité énergétique, et la réduction des impacts sur les écosystèmes et la biodiversité¹⁰.

La fiabilité peut être considérée comme une composante de l'efficacité. Une technologie est fiable si les résultats qu'elle génère ne comportent pas d'erreurs. Par exemple, une utilisation de la reconnaissance faciale dans le but d'identifier des personnes pourrait générer ce qu'on appelle des « faux positifs », c'est-à-dire qu'elle identifierait à tort une image avec le nom d'une personne, ou des « faux négatifs », c'est-à-dire qu'elle ne réussirait pas à reconnaître la personne qu'on cherche à identifier. Plus une technologie génère de faux positifs ou de faux négatifs, moins elle est fiable.

Une technologie n'a pas nécessairement à être efficace ou fiable à 100 % pour être acceptable. On peut néanmoins s'attendre à ce que l'exigence de fiabilité soit plus élevée dans le cas d'utilisations qui peuvent entraîner des préjudices aux individus, comme, par exemple, pour la surveillance policière pouvant mener à des arrestations. Dans le cas où la RF vise à effectuer le travail normalement fait par un être humain (comme pour les contrôles de sécurité), est-ce suffisant qu'elle soit aussi fiable que l'humain ? Quel devrait être le seuil

¹⁰ Voir à cet effet le principe 10 de la *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, portant sur le développement soutenable.

de fiabilité minimal pour qu'elle soit acceptable, selon les différents contextes ? Peut-on évaluer la fiabilité de manière rigoureuse ? Enfin, même si la RF était fiable à 100 %, y a-t-il des situations où son utilisation serait néanmoins inacceptable ? Pour répondre à ces questions, il faut considérer d'autres valeurs.

Égalité, équité et non-discrimination

Parmi ces autres valeurs à considérer, on retrouve celles d'égalité et d'équité. Pour simplifier, disons que l'égalité consiste à ce que chaque personne soit traitée avec la même préoccupation morale et avec le même respect¹¹. L'équité décrit plutôt une situation où le traitement accordé à différentes personnes est juste et impartial. Elle s'oppose au favoritisme, à la discrimination, etc., et exige que les disparités de traitement soient rigoureusement justifiées en des termes acceptables par tous.

Prenons l'exemple d'un processus d'embauche. Chaque personne qui postule pour l'emploi est en droit de s'attendre à être traitée de la même manière que les autres candidates et candidats, c'est-à-dire qu'elle doit avoir les mêmes chances au départ d'être sélectionnée (*égalité des chances*) et être soumise aux mêmes critères de sélection (*égalité procédurale*). Néanmoins, il est acquis qu'elle n'a pas un droit égal d'être sélectionnée pour l'emploi si elle n'a pas les compétences nécessaires ou si elle n'est pas la meilleure candidate en lice. Le critère de la compétence est acceptable pour tous et n'est donc pas un motif de discrimination illégitime. Mais si sa candidature n'est pas retenue en raison de la couleur de sa peau, il s'agit d'un cas de discrimination qui va à l'encontre de l'équité. Ainsi, un algorithme de reconnaissance faciale utilisé pour le triage de candidatures et qui aurait pour résultat de rejeter des candidatures de personnes non blanches dans une plus forte proportion que celles de personnes blanches poserait problème sur le plan de l'équité.

Ce problème est bien réel. Dans certains contextes, l'utilisation d'un système de reconnaissance faciale pourrait avoir des effets discriminatoires sur certains groupes d'individus, ce qui va à l'encontre du droit à la non-discrimination. Par exemple, plusieurs études démontrent que la reconnaissance faciale est moins fiable pour établir des correspondances lorsque les personnes visées sont non blanches, ou lorsqu'elles sont des femmes, des personnes âgées ou des enfants¹². Dans un tel cas, un problème de fiabilité entraîne un problème d'équité et de discrimination potentielle.

La discrimination liée à l'utilisation de la reconnaissance faciale, ou d'outils d'intelligence artificielle de manière générale, peut découler de biais¹³ dans les algorithmes d'intelligence artificielle. Ces biais peuvent avoir plusieurs sources. Par exemple, il est possible que les données elles-mêmes soient biaisées, entre autres parce que les données collectées ne permettent pas de bien représenter le monde. Si plus de données sont collectées sur les caucasiens que leur réelle proportion dans une communauté, il est alors possible qu'un système d'intelligence artificielle fonctionne mieux pour ces individus. Les données collectées peuvent aussi représenter des biais actuels d'un groupe d'individus, c'est-à-dire qu'elles représentent fidèlement une réalité comportant elle-même des injustices. Ces données peuvent introduire des biais dans les systèmes d'intelligence artificielle et dans les systèmes de reconnaissance faciale, surtout considérant qu'elles sont essentielles pour l'entraînement de ces systèmes.

11 Gosepath (2007).

12 Voir, entre autres, Grother et al. (2019).

13 Un biais est une déviation systématique des résultats, souvent involontaire, qui remet en cause leur validité.

Des biais peuvent aussi être introduits dans la phase de développement ou d'entraînement des systèmes d'intelligence artificielle ou de reconnaissance faciale. Dans la phase de développement des systèmes de reconnaissance faciale, il est évidemment nécessaire de faire des choix. À quoi servira ce système ? À qui sera-t-il vendu ? Quel problème ce système permettra-t-il de résoudre ? Les choix faits par rapport à ces questions, et par rapport à bien d'autres, pourraient faire en sorte que le système de reconnaissance faciale soit porteur des biais des développeurs. Une situation similaire peut survenir durant la phase d'entraînement des systèmes de reconnaissance faciale, où des développeurs doivent souvent déterminer quels attributs ou caractéristiques sont les plus importants pour que ces systèmes fonctionnent bien.

Transparence ou explicabilité des résultats

Les biais peuvent être difficiles à identifier et corriger, surtout si un système de reconnaissance faciale n'est pas transparent. Un système de reconnaissance faciale est transparent s'il est possible de suivre, de reconstruire ou de comprendre le chemin décisionnel suivi par ce système. Autrement, ce système sera dit opaque. Dans certains cas, il sera suffisant qu'un tel système soit transparent pour une personne qualifiée dans le domaine de l'IA. Dans d'autres cas, il sera nécessaire qu'un système de reconnaissance faciale soit transparent même pour une personne qui n'est pas une experte dans le domaine de l'IA, par exemple si cette personne a besoin de formuler un jugement sur les résultats obtenus par ce système en vue de donner ou non son consentement ou en vue d'exercer un recours. Le contexte influence donc grandement l'étendue de l'exigence de transparence.

Le caractère opaque des systèmes d'intelligence artificielle a maintenant droit à une expression consacrée dans les écrits : le « problème de la boîte noire ». Selon les termes de ce problème, bien qu'il soit possible d'identifier les intrants à un système d'IA (les images sur lesquelles celui-ci est entraîné) et les extrants de ce système (sa réponse à une question précise, par exemple), il n'est pas possible d'identifier ce qui se passe entre les deux. D'où l'idée qu'un système d'IA serait comme une boîte noire. Le même constat s'applique aux systèmes de reconnaissance faciale qui reposent sur l'IA pour fonctionner.

Il est toutefois possible d'outrepasser cet effet de boîte noire en développant différentes techniques qui expliquent la prise de décision d'un système de reconnaissance faciale. Ce processus d'explicabilité cherche, justement, à rendre le système de reconnaissance faciale transparent. Toutefois, il semble que, dans plusieurs cas, plus un système d'intelligence artificielle respecte ce critère d'explicabilité, moins il est précis (fiabilité). En effet, il est généralement reconnu que les algorithmes d'intelligence artificielle avec le plus grand pouvoir prédictif sont généralement les algorithmes les plus opaques. Toutefois, plusieurs techniques et solutions sont actuellement à l'essai pour rendre les systèmes d'intelligence artificielle de plus en plus transparents¹⁴. Dans tous les cas, l'enjeu de la transparence des systèmes de reconnaissance faciale soulève des questions techniques importantes. De plus, rien ne garantit qu'un utilisateur d'un tel système sera en mesure de comprendre les ramifications techniques nécessaires au fonctionnement de ce système, ce qui risque de rendre parfois difficile une utilisation responsable de la technologie de reconnaissance faciale.

14 Pour plus de détails sur ce point, voir les articles de Carabantes (2019) et Pégny et Ibnouhsein (2018).

Accès à l'information et développement des connaissances de la population

La valeur de transparence pourrait aussi être entendue au sens de la transparence du contexte d'utilisation. Dans ce cas, ce sont les conditions d'utilisation d'un système qui sont transparentes, c'est-à-dire qu'une information adéquate concernant la nature, les visées et les implications de l'utilisation de ce système est facilement accessible et compréhensible. Par exemple, si un centre commercial utilise un système de reconnaissance dans le but véritable de surveiller les consommateurs et de développer des profils précis de consommation, l'utilisation de ce système sera transparente si cette information est fournie aux individus touchés par l'utilisation de cette technologie. Pour différencier cette dernière définition de celle de la transparence comme explicabilité, les termes d'accessibilité de l'information concernant les utilisations sont préférés ici.

L'actualisation de cette valeur se heurte à un manque de connaissances et de compétences numériques au sein de la population, qui doit de plus en plus composer avec des environnements technologiques très complexes et difficilement compréhensibles, voire carrément opaques, comme il vient d'être mentionné. Au « problème de la boîte noire » vient alors s'ajouter celui de la « fracture numérique », c'est-à-dire les inégalités prévalant entre les individus en ce qui concerne l'accès aux technologies numériques, dont fait partie la reconnaissance faciale, ainsi qu'aux connaissances et compétences nécessaires pour en comprendre les ressorts, en tirer avantage et en éviter les pièges.

De plus, dans le domaine du numérique, les conditions d'utilisation sont généralement présentées dans des documents volumineux, elles sont formulées dans un langage complexe empruntant aux jargons technique et juridique, et elles sont conséquemment rarement lues et comprises par les utilisateurs. Cela pose problème sur le plan de l'éthique, car une véritable accessibilité et intelligibilité de l'information est une condition nécessaire pour assurer la légitimité des actions posées par les acteurs faisant usage des technologies, pour maintenir la confiance du public et pour favoriser l'autonomie des personnes soumises à ces technologies (leur capacité à faire des choix éclairés). Comme le soulignait déjà la CEST-Jeunesse 2018, qui s'est penchée sur la notion de citoyenneté à l'ère du numérique, « la transparence [du contexte d'utilisation] n'exige pas uniquement que l'information soit *disponible*, elle doit être réellement *accessible*. Cela veut dire qu'elle doit être compréhensible et qu'il doit être possible d'en prendre connaissance dans un temps raisonnable »¹⁵.

Autonomie des individus

L'autonomie est « la liberté de décider et d'agir pour soi-même, ce qui suppose [...] la possibilité de prendre une décision libre et éclairée, conforme à ses valeurs, et qui donne sens à son geste¹⁶ ». Respecter l'autonomie de l'individu, c'est protéger ce dernier contre l'ingérence induite des autres dans la conduite de sa vie, ou contre des politiques répressives ou arbitraires, par exemple.

¹⁵ Commission de l'éthique en science et en technologie (2018, p. 13).

¹⁶ Commission de l'éthique en science et en technologie (2016, p. 16).

Une manière dont l'autonomie individuelle est protégée dans nos sociétés est par l'entremise d'une exigence de consentement de la part des individus, c'est-à-dire d'obtenir l'autorisation des personnes concernées avant de poser une action qui mette en jeu leur intégrité physique ou psychologique, leur vie privée, ou toute autre chose qui les affecte au plus haut point¹⁷. Sur la base de ce principe, une personne devrait pouvoir être en mesure d'accepter ou de refuser l'utilisation de la reconnaissance faciale sur sa personne.

Il est cependant complexe de toujours appliquer les critères nécessaires à un consentement valide, qui requiert la possibilité de prendre une décision libre et éclairée. Par exemple, comme il a été mentionné précédemment, il peut être très difficile pour l'individu d'avoir un niveau de compréhension de la technologie et de ses implications qui soit suffisant pour que la décision soit vraiment éclairée. Aussi, si la reconnaissance faciale est utilisée à des fins de sécurité, pour prévenir des crimes ou pour résoudre ceux-ci, demander le consentement peut venir contrecarrer les bienfaits potentiels liés à ce type d'utilisation.

La CEST-Jeunesse reconnaît toutefois qu'il est nécessaire d'appliquer ces critères lorsque la reconnaissance est utilisée à des fins commerciales. Dans ce cas, les individus devraient pouvoir avoir accès à une information de qualité quant à l'utilisation de la reconnaissance faciale, aux données qui sont collectées sur eux, aux usages de ces données, etc. Avoir accès à cette information de qualité et véridique est nécessaire pour qu'ils puissent consentir de manière éclairée. Ils devraient également avoir le droit de retirer leur consentement à tout moment.

Outre la question du consentement, d'autres situations peuvent mettre en jeu la valeur d'autonomie. Par l'utilisation d'un système de reconnaissance faciale, il pourrait être possible d'influencer indûment et de manière systématique les décisions des individus. Bien que les stratégies actuelles de vente permettent déjà d'influencer les décisions des individus, la reconnaissance faciale pourrait permettre de perfectionner significativement ces stratégies, principalement en fournissant de nouvelles données sur la manière dont les individus réagissent à des offres, des produits, etc. Un tel phénomène pourrait grandement participer à réduire l'autonomie d'un individu, c'est-à-dire la capacité qu'a ce dernier de faire des choix pour lui-même, selon ses propres valeurs, croyances, préférences, désirs, etc.

Protection de la vie privée

La protection de l'autonomie des individus est liée à la protection de leur vie privée. En effet, cette dernière peut être conçue comme la garantie d'un espace de liberté et d'intimité qui échappe au contrôle d'autrui et protège l'individu de l'ingérence indue des autres. Dans notre cadre juridique, la protection de la vie privée repose fortement sur la protection des renseignements personnels, c'est-à-dire des renseignements (données, informations, etc.) qui permettent d'identifier une personne. Les questions relatives à la vie privée concernent ainsi principalement le droit de regard et de contrôle qu'a l'individu sur l'acquisition, par un tiers, d'information de nature privée, sur les fins auxquelles cette information peut être utilisée et sur l'étendue du partage qui peut en être fait.

La collecte de données sur les individus et l'utilisation de la reconnaissance faciale permettent de suivre les individus et leurs déplacements dans des espaces publics, ce qui soulève des enjeux liés à la surveillance des individus en question. Faites à l'insu des personnes ciblées, elles soulèvent en plus des enjeux en matière de transparence, de consentement et de respect de l'autonomie des personnes. De plus, le seul sentiment d'être surveillé peut être suffisant pour avoir un effet d'inhibition sur les individus, par lequel le champ des

¹⁷ Sous réserve de certaines contraintes légales.

actions (légales) qu'ils se sentent à l'aise de poser est rétréci, ce qui constitue une contrainte psychologique à leur liberté. Des effets sur la santé mentale ont aussi été démontrés, un contexte de surveillance entraînant plus de stress, d'anxiété et de dépression, entre autres, au sein de la population cible¹⁸.

En outre, la reconnaissance faciale permet, du moins potentiellement, une surveillance plus intrusive de ces individus, surtout si des technologies d'analyse des émotions sont également utilisées. Grâce à ces technologies, il serait en effet possible d'inférer les émotions vécues par un individu à un moment précis. Ces technologies peuvent être utilisées à des fins commerciales pour mieux comprendre les réactions émotionnelles des consommateurs devant un produit, mais aussi à des fins de sécurité pour tenter de mieux prévenir les crimes. Ce qui est en jeu ici, c'est le droit à l'intériorité de la personne, compris comme étant le droit de protéger son autonomie en ce qui concerne ce qu'elle choisit d'exprimer explicitement, et à qui, de ses émotions, sentiments, réflexions et croyances (ce qui se passe « à l'intérieur d'elle »)¹⁹.

Sera-t-il toujours possible de savoir quelles données sont collectées ? Est-ce qu'il y a des situations où il serait acceptable de ne pas savoir quelles données sont collectées ? Sera-t-il toujours possible de savoir quelles utilisations, dont les utilisations secondaires, seront faites de ces données ? Toutes ces questions, toutefois, ne sont pas nécessairement propres à la reconnaissance faciale, mais bien à toutes ces technologies qui permettent de collecter des données sur les individus.

Sécurité

Plusieurs applications de reconnaissance faciale visent explicitement la promotion de la sécurité des personnes, des collectivités ou des organisations. Selon la définition qu'en propose l'Organisation mondiale de la santé :

La sécurité est un état où les dangers et les conditions pouvant provoquer des dommages d'ordre physique, psychologique ou matériel, sont *contrôlés* de manière à préserver *la santé et le bien-être* des individus et de la communauté. C'est une *ressource* indispensable à la vie quotidienne qui permet à l'individu et à la communauté de réaliser ses aspirations.²⁰

À ce titre, la sécurité fait l'objet de garanties constitutionnelles et est inscrite – sur le même pied que la vie, la liberté, l'intégrité ou la dignité – comme un droit fondamental dans la *Charte des droits et libertés de la personne* du Québec (article 1) et la *Charte canadienne des droits et libertés* (article 7)

On reconnaît à la sécurité deux dimensions²¹. La première est objective et fait intervenir des paramètres permettant de mesurer le degré de sécurité réel ou l'absence de menaces ou de dangers. La seconde est subjective et renvoie davantage au sentiment que les personnes éprouvent par rapport à leur sécurité. Ces deux dimensions s'influencent mutuellement et sont également nécessaires pour qualifier une situation de « sécuritaire ». En ce sens, l'amélioration et le maintien du bien-être et de la santé de la population reposent au moins en partie sur un haut niveau de sécurité *réelle* et de sécurité *perçue*.

18 Voir notamment Subasic et al. (2011) ainsi que Smith et al. (1992).

19 Voir Champagne (2018a).

20 OMS (1998, p. 8), les italiques sont présents dans le texte original.

21 Voir Commission de l'éthique en science et en technologie (2008, p. 3).

La CEST-Jeunesse souligne une certaine tension entre la sécurité, d'une part, et la liberté, l'autonomie et la protection de la vie privée des individus, d'autre part. En effet, l'utilisation de la reconnaissance faciale pourrait permettre, dans certains contextes, d'augmenter le sentiment de sécurité des individus plus vulnérables. Il existe toutefois une tension entre la protection de certains individus, d'un côté, et l'empiétement sur la liberté de tous, de l'autre.

Liberté économique des entreprises et des consommateurs

Dans notre système économique, il est reconnu aux individus la liberté de prendre les moyens (légaux) qu'ils jugent opportuns pour entreprendre une activité dans le but de générer un profit et de récolter les fruits de leurs efforts d'entrepreneuriat. Autrement dit, notre société reconnaît comme légitimes et promeut les valeurs de liberté économique – la capacité de choisir et d'entreprendre des actions économiques (faire des transactions, acquérir des technologies, etc.) et de rechercher la profitabilité – et de rétribution au mérite – la rétribution positive (gain) et négative (perte) en fonction du travail, de l'effort et de l'habileté²².

Concernant le développement de la reconnaissance faciale, qu'est-il légitime d'imposer comme réglementations à l'entreprise, dans le respect de sa liberté économique, de sa profitabilité ou de son attente d'un retour sur investissement? Comment permettre au secteur privé de participer à l'innovation et au développement technologiques, sans néanmoins entraîner d'effets négatifs sur les plans social et éthique? La liberté économique des entreprises peut-elle entrer en conflit avec la liberté des consommateurs (autonomie) ou avec les intérêts économiques des individus dont les données personnelles sont utilisées par des tiers pour générer un profit? Les revenus tirés de l'utilisation de données collectées auprès de personnes soumises à la reconnaissance faciale devraient-ils être redistribués partiellement ou même entièrement à ces personnes?

Développement économique et prospérité

L'action économique des acteurs privés peut aussi être évaluée au regard de leur participation au développement économique et à la prospérité collective (maximisation des bénéfices totaux). Le développement du secteur des technologies de reconnaissance faciale devrait-il être orienté dans l'optique d'un développement local et de la création de richesses sur le territoire québécois? La compétitivité du Québec sur les marchés internationaux serait-elle compromise s'il tarde à investir dans ces technologies? Risque-t-on alors de dépendre d'entreprises étrangères au moment d'acquérir et de faire usage de ces technologies, sans pouvoir alors tirer parti des bénéfices ou participer aux processus décisionnels qui concourent à leur développement?

Dans les dernières années, les secteurs public et privé se sont alliés pour faire de Montréal un pôle de développement de l'intelligence artificielle, un ensemble de technologies dont dépendent les applications de reconnaissance faciale. Selon les données fournies par le ministère de l'Économie et de l'Innovation du Québec, ce sont plus de 2,3 milliards de dollars qui ont été annoncés ou ont été rendus disponibles pour la recherche, le développement de technologies ou l'adoption de solutions d'intelligence artificielle au Québec²³. Que devrait pouvoir exiger l'État de la part des chercheurs et des entreprises qui reçoivent des fonds publics dans le cadre des multiples programmes de subvention qui ont été mis sur pied?

²² Voir Commission de l'éthique en science et en technologie (2016, p. 47).

²³ Ministère de l'Économie et de l'Innovation (2020).

De manière plus fondamentale encore, on peut se demander comment comparer les gains et les pertes économiques associés au développement d'un secteur technologique avec les avantages et les risques sur les plans social et éthique. Par exemple, jusqu'à quel point est-on prêt à sacrifier certaines valeurs comme la protection de la vie privée pour pouvoir profiter, en contrepartie, des bénéfices économiques liés au développement de la reconnaissance faciale ?

Environnement et développement durable

Les technologies entraînent des conséquences pour les personnes, les groupes et les sociétés, mais aussi pour l'environnement. Ces conséquences doivent être prises en considération dans l'évaluation de l'acceptabilité d'une technologie. Au regard de la crise climatique, une telle évaluation des conséquences environnementales est encore plus cruciale. En effet, l'augmentation des émissions de gaz à effet de serre (GES) participe aux changements climatiques mettant en danger la vie et la santé humaines, ainsi que l'intégrité des écosystèmes et la biodiversité²⁴. Dans ce contexte, le développement des technologies et leur utilisation devraient idéalement contribuer à réduire l'empreinte carbone de l'humanité, plutôt que de l'accroître.

Or, les technologies d'intelligence artificielle sur lesquelles repose la reconnaissance faciale ont un bilan carbone plutôt controversé. Une étude récente évalue que l'entraînement d'un seul système d'IA (apprentissage profond) émettrait jusqu'à 284 tonnes de carbone, soit cinq fois plus que ce qui est émis par une voiture pendant toute sa durée de vie, incluant sa fabrication²⁵. Il y a donc, pour la RF, un enjeu de développement durable, c'est-à-dire d'un développement qui puisse être réalisé de manière responsable sur les plans économique, social et environnemental. Au Québec, les principes de développement durable, dont la protection de l'environnement, sont enchâssés dans la *Loi sur le développement durable*.

Responsabilité et imputabilité

La responsabilité peut s'entendre de multiples manières. On dit parfois d'une personne qu'elle est responsable lorsqu'elle agit de manière raisonnable ou lorsqu'elle prend rigoureusement en compte les incidences que peuvent avoir ses actions sur autrui. On dit aussi qu'une personne est responsable d'une certaine situation si elle en est la cause ou si elle avait une obligation d'agir d'une certaine manière pour qu'advienne cette situation ou pour éviter qu'elle se produise. On dit enfin qu'une personne est responsable si elle peut être blâmée lorsque ses actions causent des torts, voire être tenue de compenser les personnes qui ont subi ces torts (imputabilité).

Dans le cas qui occupe la CEST-Jeunesse, ces valeurs sont au cœur de questions telles que : Qui est ou devrait être responsable des résultats obtenus au moyen d'une technologie de reconnaissance faciale ? Est-ce qu'un algorithme peut être tenu responsable ? Quelles sont les obligations des différents acteurs qui développent, commercialisent ou utilisent la reconnaissance faciale ? L'État devrait-il exiger à ces acteurs de rendre des comptes et, si oui, de quelle manière ?

24 GIEC (2018).

25 Lu (2019).

Indépendance des institutions publiques et bien commun

Une institution publique répond à des exigences particulières, ce qui fait en sorte qu'elle ne peut avoir le même rapport avec ses citoyens qu'une entreprise privée avec ses clients. Les citoyens ne concluent pas un contrat de service avec un « État-fournisseur », mais sont d'emblée soumis au pouvoir public. Ainsi, l'autorité publique doit répondre à des exigences de légitimité démocratique. Les institutions publiques doivent faire preuve de responsabilité et maintenir le lien de confiance avec le public, ce qui passe de plus en plus par la transparence des processus décisionnels. L'action publique doit être menée dans l'intérêt du bien commun et dans un esprit d'inclusion.

Cela se matérialise par divers principes, tels que l'autonomie de la sphère publique par rapport aux intérêts privés, ainsi que le primat de l'intérêt public sur les intérêts privés dans la prise de décision des gouvernements et des institutions publiques. Cela implique d'assurer des bénéfices pour la collectivité ou, dit autrement, d'éviter que les coûts et inconvénients d'une mesure soient principalement à la charge du secteur public, alors que les bénéfices soient récoltés par le secteur privé (dimension d'équité), comme il peut arriver lorsqu'un secteur d'activité économique est fortement subventionné.²⁶

Le développement des nouvelles technologies, dont l'intelligence artificielle et plus spécifiquement la reconnaissance faciale, peut être très coûteux et requiert une expertise poussée en programmation informatique. Les compagnies privées sont donc la plupart du temps en meilleure position que les organismes publics et le gouvernement pour développer ces technologies, même si la recherche en intelligence artificielle repose actuellement en partie sur des investissements publics²⁷. Les entreprises privées sont souvent en meilleure position pour attirer l'expertise nécessaire à ce développement, entre autres parce qu'elles peuvent plus facilement répondre aux demandes salariales des travailleurs dont l'expertise est recherchée ou rare. Ces facteurs participent à mettre les organismes publics dans une position de vulnérabilité lorsqu'il s'agit d'acquérir ces nouvelles technologies. Cette position de vulnérabilité a une répercussion négative sur leur autonomie et indépendance.

Par exemple, si un organisme public est à la recherche d'un système d'intelligence artificielle et qu'il lance un appel d'offres, une entreprise privée qui répond à cet appel pourrait profiter du manque d'expertise au sein de cet organisme pour faire miroiter des fonctionnalités qui ne sont pas réellement utiles, qui ne permettent pas de remplir les objectifs visés par l'organisme public, etc. Ce manque d'expertise au sein des organismes publics pourrait également creuser l'asymétrie de l'information qui existe entre ce que la compagnie qui vend un système de reconnaissance faciale sait à propos de ce système et ce que l'acheteur sait à propos de celui-ci. Dans une telle situation, il est probable qu'un organisme public se retrouve à payer plus qu'il l'aurait fallu pour un système de reconnaissance faciale, ou qu'il paie pour un système qui ne correspond pas réellement ou complètement à ce qu'il cherche. Dans une telle situation, il devient alors difficile de réaliser les bénéfices collectifs liés à l'utilisation de la reconnaissance faciale, ce qui entre en tension avec une certaine conception de la prospérité.

²⁶ Cette analyse est reprise de l'avis de la Commission de l'éthique en science et en technologie (2017b).

²⁷ Ministère de l'Économie et de l'Innovation (2020).

3

Analyse et recommandations

Il est difficile de déterminer une valeur ou un ensemble de valeurs qui aurait préséance dans l'ensemble des situations de manière à formuler une solution générale aux enjeux soulevés par la reconnaissance faciale. Néanmoins, les délibérations de la CEST-Jeunesse ont permis d'établir certaines priorités.

Tout d'abord, ses membres ont abordé les enjeux au travers du prisme de la protection des droits et libertés de la personne, avec un accent mis sur l'égalité et la non-discrimination, et ce, en portant une attention particulière au sort des personnes plus vulnérables. Sous cette étiquette se retrouvent aussi le respect de l'autonomie, principalement au moyen de l'exigence de consentement, ainsi que la protection du droit à la vie, à la sécurité et à l'intégrité des personnes, conçue comme une condition nécessaire de l'exercice de l'autonomie.

Ensuite, la CEST-Jeunesse a privilégié une approche basée à la fois sur le développement des connaissances au moyen de l'éducation, de la sensibilisation du public et de la recherche scientifique, d'une part, et sur la responsabilisation des acteurs au moyen de mesures visant à assurer l'imputabilité face aux risques posés par la reconnaissance faciale.

Enfin, elle reconnaît l'importance de garantir l'indépendance des institutions publiques face aux différents intérêts privés, de manière à orienter le développement et l'encadrement de la reconnaissance faciale dans l'intérêt public, tout en soulignant que ces institutions doivent elles-mêmes être soumises à cet encadrement.

Consentement et droit de refus



Les textes des conditions d'utilisation des technologies du numérique, dont celles de la reconnaissance faciale, sont souvent complexes. Cette complexité est parfois due à la forme dans laquelle se présentent les conditions d'utilisation : taille de la police, longueur du document, etc. D'autres fois, cette complexité est plutôt due au contenu comme tel, ces conditions étant souvent écrites dans un langage juridique difficile à comprendre pour un non initié. Cette complexité des conditions d'utilisation soulève des enjeux concernant la qualité de l'information transmise aux individus visés par l'utilisation de la reconnaissance faciale, en plus de la facilité de compréhension de cette information. Cette situation rend, souvent, difficile le consentement libre et éclairé.

La *Loi sur la protection des renseignements personnels dans le secteur privé* plus spécifiquement l'article 14, prévoit déjà que le consentement doit être demandé lorsqu'il y a collecte de données sur les individus. La CEST-Jeunesse tient à rappeler cette exigence qui s'applique au secteur privé.

Rappel 1

Le consentement doit être explicitement demandé lorsqu'il y a collecte de renseignements personnels sur les individus, lorsqu'il y a communication ou utilisation d'un renseignement personnel qui n'a pas été établi au préalable.

Toutefois, l'utilisation de la reconnaissance faciale est aussi possible même sans collecte de données qui permettent d'identifier des individus. En effet, avec la reconnaissance faciale, il est possible de collecter des renseignements sans que ceux-ci soient des renseignements personnels : une réaction émotionnelle à une publicité, par exemple. Une telle réaction ne permettant pas d'identifier un individu en particulier, elle n'est pas considérée comme un renseignement personnel. Toutefois, rien n'empêche qu'une telle utilisation de la

reconnaissance faciale puisse avoir des effets sur l'intégrité physique et, surtout, morale d'une personne. Pour prévenir ce type de situations, la CEST-Jeunesse considère qu'il est préférable que toute utilisation de la reconnaissance faciale nécessite le consentement, que des renseignements personnels soient collectés ou non.

Recommandation 1

Que les individus puissent, dans la mesure du possible, consentir à l'utilisation de la reconnaissance faciale.

Cette recommandation est à portée générale, c'est-à-dire qu'elle s'applique autant aux gouvernements qu'aux entreprises privées. D'abord, le Gouvernement du Québec pourrait imposer des normes communes pour que les individus puissent consentir à l'utilisation de la reconnaissance faciale. Ensuite, les entreprises privées ont également la responsabilité de veiller à ce que toutes les personnes touchées par l'utilisation d'une telle technologie y consentent.

La CEST-Jeunesse rappelle également les conditions qui doivent être réunies pour qu'un consentement à l'utilisation de la reconnaissance faciale puisse être considéré comme étant valide. Ces conditions se trouvent dans l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, et explicitées dans le rapport quinquennal 2016 de la Commission d'accès à l'information²⁸ :

- Le consentement doit être **manifeste**, c'est-à-dire évident, certain et indiscutable ;
- Le consentement doit être **libre**, c'est-à-dire être donné sans contrainte ;
- Le consentement doit être **éclairé**, c'est-à-dire qu'il doit être précis, rigoureux et spécifique ;
- Le consentement est également donné à des **fins spécifiques** et pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé ;
- Le consentement doit être **continu**, c'est-à-dire qu'il doit pouvoir être retiré à tout moment et que, pendant tout le temps où les données sont conservées ou utilisées, toute information pertinente doit être communiquée aux personnes ayant donné leur consentement.

Un consentement qui ne respecterait pas un de ces critères (qui ne serait pas manifeste, par exemple) doit être considéré comme nul.

Dans certaines situations, il est possible que la seule manière de préserver l'intégrité physique et morale de la personne, ou bien de favoriser la liberté de choix et l'autonomie, soit de donner un droit de refus pour que tout individu puisse refuser d'être sujet à un système de reconnaissance faciale sans subir de conséquences liées à ce choix. Par exemple, pouvoir entrer dans un centre commercial ne devrait pas dépendre d'une acceptation à se soumettre à de la reconnaissance faciale. Dans une telle situation, chaque personne devrait pouvoir côtoyer ce lieu sans avoir à se soumettre à l'utilisation d'une telle technologie. Cette possibilité de refuser l'utilisation de la reconnaissance faciale est ce que la CEST-Jeunesse comprend comme étant un droit de refus.

²⁸ Commission d'accès à l'information (2016, p. 91-93).

Recommandation 2

Que les individus puissent, dans la mesure du possible, refuser d'être sujet à un système de reconnaissance faciale et, ceci, sans conséquences.

Évidemment, dans certaines situations, surtout lorsque la reconnaissance faciale est utilisée à des fins de sécurité, il ne sera pas possible d'attribuer un tel droit à quiconque. Faire cela viendrait annuler les bénéfices potentiels liés à l'utilisation de la reconnaissance faciale. Toutefois, lorsque la reconnaissance faciale est utilisée, par exemple, à des fins commerciales, un tel droit de refus pourrait être accordé sans que cela vienne contredire les raisons qui motivent le recours à cette technologie.

Sécurité



Bien qu'il ne soit pas possible d'attribuer un droit de refus lorsque la reconnaissance faciale est utilisée à des fins de sécurité, cela ne veut pas dire que l'utilisation de la reconnaissance à ces fins ne doit pas être balisée.

Parmi ces balises, la CEST-Jeunesse souligne l'importance de toujours utiliser la reconnaissance faciale dans le respect des libertés fondamentales et des droits fondamentaux reconnus dans la *Charte canadienne des droits et libertés* et dans la *Charte des droits et libertés de la personne* du Québec. Plus particulièrement, la CEST-Jeunesse veut mettre l'accent sur la protection des personnes en situation de vulnérabilité et des groupes marginalisés. Mieux protéger ces personnes et ces groupes pourrait ainsi être un des objectifs visés par l'utilisation de la reconnaissance à des fins de sécurité. De plus, l'utilisation de la reconnaissance faciale à des fins de sécurité doit répondre à certains critères, dont son efficacité, sa nécessité et sa proportionnalité. Autrement, on risque de voir des dérives liées à une surveillance excessive des individus, autant de la part des organismes publics que privés.

Recommandation 3

Que l'utilisation de la reconnaissance faciale à des fins de sécurité soit justifiée par son efficacité, sa nécessité et sa proportionnalité.

De plus, la CEST-Jeunesse rappelle, tel que spécifié dans l'article 7 de la *Charte des droits et libertés de la personne* du Québec, que la demeure est inviolable, en ce sens qu'elle appartient entièrement à la sphère privée des individus. Évidemment, il existe des exceptions à cette inviolabilité du domicile, telles que reconnues dans certains articles du *Code criminel* canadien²⁹.

Rappel 2

À l'exception des conditions et des exceptions reconnues par le Code criminel canadien, la demeure est inviolable et le Gouvernement du Québec et ses organismes, ainsi que les entreprises privées, ne peuvent utiliser les technologies de la reconnaissance faciale pour s'immiscer dans celle-ci sans le consentement exprès de la personne résidente.

²⁹ À ce sujet, voir la partie 6 du Code criminel.

Éducation et sensibilisation



Pour que le consentement à l'utilisation de la reconnaissance faciale puisse réellement être éclairé, les individus doivent pouvoir savoir à quoi ils consentent. Les circonstances font souvent en sorte que les individus ne savent pas à quoi ils consentent. Parfois, cela est dû à l'absence d'une information facilement accessible, claire, intelligible ou véridique. À ce sujet, la CEST-Jeunesse considère important de souligner que les organismes qui utilisent la reconnaissance devraient toujours rendre cette information facilement accessible au public. Celle-ci devrait aussi être rédigée dans un langage clair et intelligible, de sorte que le plus grand nombre possible d'individus puissent bien saisir, rapidement, ce à quoi ils consentent. Par exemple, il pourrait s'agir de mettre l'accent sur les quelques éléments les plus importants à savoir et dont la prise de connaissance ne devrait prendre que quelques dizaines de secondes, voire quelques minutes. De plus, cette information devrait être véridique et inclure tout élément essentiel à un consentement valide. En effet, un individu ne peut pas consentir de manière libre et éclairé si un organisme public ou si une entreprise privée lui cache de l'information à propos d'une utilisation spécifique de la reconnaissance faciale.

D'autres fois, les conditions nécessaires à un réel consentement ne sont pas réunies parce que les individus n'ont pas une connaissance appropriée du fonctionnement d'une technologie, des bénéfices ou des risques associés à celle-ci. Une meilleure connaissance à ce sujet pourrait favoriser un consentement libre et éclairé quant à l'utilisation des technologies de reconnaissance faciale.

Recommandation 4

Par l'élaboration d'outils d'éducation et de sensibilisation, le Gouvernement du Québec doit informer le public, plus particulièrement les jeunes, du fonctionnement de la reconnaissance faciale, ainsi que des bénéfices et des risques associés à l'utilisation de cette technologie.

Pour ce faire, le Gouvernement du Québec pourrait mandater un ou plusieurs organismes pour développer ces outils d'éducation et de sensibilisation. La CEST-Jeunesse met également l'accent sur l'importance d'inclure dans le cursus scolaire des élèves québécois, d'une manière ou d'une autre, des éléments concernant le fonctionnement de la reconnaissance faciale et des autres technologies de l'intelligence artificielle, et des bénéfices et des risques associés à ces différentes technologies. Ceci pourrait cependant prendre différentes formes, dont des conférences ou des ateliers donnés par des organismes reconnus et compétents.

Responsabilité et imputabilité



Les systèmes d'intelligence permettent, entre autres, d'automatiser la prise de décision. En ce qui concerne la reconnaissance faciale, il serait possible, par exemple, d'automatiser la prise de décision sur qui peut avoir accès à un édifice ou à un lieu. Il s'agit, dans un tel cas, de s'appuyer sur les données biométriques qui permettent d'identifier un individu pour déterminer si celui-ci peut avoir accès à un lieu. Essentiellement, il s'agit donc d'automatiser une décision qui pourrait être prise par un être humain, par exemple un garde de sécurité qui authentifie qu'une personne est bien celle qu'elle prétend être en comparant le visage de celle-ci à la photo se trouvant sur une carte d'identité ou dans une base de données.

Lorsqu'il s'agit de situations où il y a un préjudice possible, que celui-ci soit entraîné directement ou indirectement par l'utilisation de cette technologie, la CEST-Jeunesse est d'avis que cette utilisation ne devrait pas venir remplacer l'être humain dans la chaîne de décision. En d'autres termes, dans une telle situation, la décision finale devrait toujours être prise par un être humain. Le système de reconnaissance faciale pourrait malgré tout être utilisé pour formuler une recommandation à un être humain, pour alimenter cette décision ou pour fournir de meilleures données probantes, mais cet être humain doit toujours être maintenu dans la boucle. Une telle option garantit qu'une personne humaine sera responsable et imputable des décisions prises, même si celles-ci l'ont été sur la base d'une recommandation venant d'un outil de reconnaissance faciale.

Recommandation 5

Que dans les cas où il y a un préjudice possible, la reconnaissance faciale demeure un outil qui soutient la décision d'un être humain et que celui-ci, ou tout autre être humain, soit toujours impliqué.

D'ailleurs, la CEST-Jeunesse suggère que le Gouvernement du Québec initie une réflexion sur les meilleures pratiques internationales en matière de gestion des données personnelles et d'encadrement de la reconnaissance faciale, pour s'inspirer de ce qui se fait de mieux à l'international.

Au-delà des résultats de cette réflexion, la CEST-Jeunesse souligne fortement que le Gouvernement du Québec devrait se doter d'une instance qui a pour principale mission de surveiller et de réguler les développements technologiques liés à l'intelligence artificielle, dont ceux en reconnaissance faciale. Cette instance pourrait par exemple mettre sur pied un système de dépôt et d'archivage des algorithmes d'intelligence artificielle, ce qui pourrait permettre de développer une meilleure connaissance des technologies de l'intelligence artificielle et des bénéfices et des risques associés à celles-ci.

Recommandation 6

Que le Gouvernement du Québec se dote d'une instance de surveillance et de régulation en matière d'intelligence artificielle.

De cette manière, le Gouvernement du Québec pourrait montrer l'exemple à l'échelle internationale en étant un précurseur en encadrement de l'intelligence artificielle.

Certaines situations problématiques surviennent aussi du fait que les développeurs des systèmes d'intelligence artificielle ne sont soumis à aucune obligation professionnelle. De cette manière, même si le développement de l'intelligence artificielle, dont la reconnaissance faciale, peut être mené par des individus bien intentionnés, très peu d'encadrement existe. Certaines entreprises privées ou certains chercheurs vont, entre autres par conviction éthique, refuser de participer à certains projets ou refuser de développer certains produits. C'est le cas par exemple pour les systèmes d'intelligence artificielle qui pourraient être utilisés en situation de conflits armés : plusieurs chercheurs et entreprises refusent de participer à de tels projets³⁰. Parfois, c'est même les employés de certaines entreprises qui font valoir leur désaccord avec les projets proposés ou acceptés par l'administration de leurs entreprises³¹. Toutefois, aucun encadrement, que ce soit déontologique ou juridique, ne régit le développement spécifique de l'intelligence artificielle par les programmeurs informatiques ou par les autres acteurs essentiels au développement de cette technologie.

³⁰ Radio-Canada (2018).

³¹ Massoud (2018).

C'est dans ce contexte que la CEST-Jeunesse considère nécessaire que le Gouvernement du Québec cherche à établir des normes qui seraient imposées autant aux développeurs et utilisateurs d'algorithmes de reconnaissance faciale, voire d'algorithmes d'intelligence artificielle tout simplement. L'objectif de telles normes serait de protéger la population québécoise de biais ou de préjudices possibles, et ainsi tenter de minimiser les situations discriminatoires liées à l'utilisation de la reconnaissance faciale. Ces normes pourraient aussi veiller à ce que le développement de l'intelligence artificielle et de la reconnaissance faciale soit respectueux de l'environnement et des principes du développement durable.

Recommandation 7

Que le Gouvernement du Québec travaille à établir des normes qui seraient imposées aux développeurs et utilisateurs d'algorithmes de reconnaissance faciale, dont un processus d'homologation obligatoire pour les applications utilisées sur le territoire québécois.

Cette recommandation peut aussi être comprise comme s'appliquant à tous les algorithmes d'intelligence artificielle, et non uniquement à ceux utilisés dans le contexte de la reconnaissance faciale.

Ce processus d'homologation viserait à assurer la conformité de chaque application à des exigences strictes en matière de fiabilité, d'équité, de respect de la vie privée et de responsabilité environnementale. Il pourrait être en partie ou en totalité mené par des comités d'éthiques multidisciplinaires, diversifiés, indépendants et avec une expertise suffisante en intelligence artificielle. L'indépendance des comités d'éthique est importante pour outrepasser les limites intrinsèques aux comités d'éthique internes aux entreprises et organismes, qui peuvent être en conflit d'intérêts lors de l'évaluation des algorithmes de reconnaissance faciale ou d'intelligence artificielle.

Finalement, la CEST-Jeunesse considère que des normes claires et strictes devraient être établies par le Gouvernement du Québec pour encadrer l'intégration des technologies de la reconnaissance faciale dans les appareils intelligents ou dans les objets connectés, surtout ceux qui pourraient être utilisés par les mineurs ou qui sont directement développés pour ce marché (les jouets connectés, par exemple). Ces normes devraient viser, entre autres, à protéger la vie privée des consommateurs. L'Office de la protection du consommateur pourrait être mandaté pour faire appliquer et respecter ces normes.

Recommandation 8

Que des normes strictes soient élaborées par le Gouvernement du Québec pour encadrer l'intégration de la reconnaissance faciale dans les appareils intelligents mis en marché par le secteur privé.

Recherche



La recherche en intelligence artificielle dépend grandement des fonds publics, entre autres parce que cette recherche peut s'avérer très dispendieuse, mais surtout parce que rien ne garantit que la recherche en intelligence artificielle soit profitable. C'est surtout vrai pour la recherche fondamentale, qui est pourtant essentielle pour que des applications plus techniques ou utiles puissent voir le jour. Ainsi, les entreprises privées sont parfois réfractaires à investir des sommes importantes en recherche. Pour veiller à ce que les bénéfices liés au développement de l'intelligence artificielle puissent se réaliser, les gouvernements sont donc enclins à investir des sommes importantes pour la recherche.

La CEST-Jeunesse souligne que ces organismes publics devraient continuer de veiller à ce que les bénéfices liés au développement de l'intelligence artificielle et de la reconnaissance faciale ne soient pas uniquement privés, mais qu'ils soient plutôt redistribués à l'ensemble de la collectivité. Ceci vaut pour les bénéfices qui sont monétaires, mais aussi pour tout autre type de bénéfices. Ce financement octroyé à la recherche en intelligence artificielle devrait aussi viser à développer une expertise québécoise en matière d'intelligence artificielle. Cette expertise québécoise pourrait être composée de chercheurs universitaires des différentes universités du Québec, des entreprises québécoises, mais aussi des membres des ministères et organismes du Gouvernement du Québec.

Recommandation 9

Que le ministère de l'Économie et de l'Innovation et les Fonds de recherche du Québec instaurent un programme de financement de la recherche sur l'IA et la reconnaissance faciale au bénéfice de l'ensemble de la population québécoise.

La CEST-Jeunesse souligne aussi que le Gouvernement du Québec pourrait évaluer les outils fiscaux à sa disposition pour assurer une certaine redistribution à l'ensemble de la collectivité des bénéfices issus de l'utilisation de la reconnaissance faciale. La possibilité de générer ainsi de nouveaux revenus pour l'État ne devrait toutefois pas servir ensuite à justifier une utilisation accrue des technologies de la reconnaissance faciale.

Indépendance des institutions publiques



Les ministères et organismes du Gouvernement du Québec, ainsi que d'autres organismes publics, pourraient vouloir utiliser des systèmes de reconnaissance faciale pour des objectifs tout à fait justifiés, respectables ou louables. Par exemple, un organisme public pourrait vouloir se procurer un système de reconnaissance faciale pour sécuriser l'accès à un lieu contenant des dossiers confidentiels. Mais si cet organisme ne possède aucune expertise interne en matière de développement de l'intelligence artificielle, ou d'achat de logiciel de reconnaissance faciale, il est possible que des acteurs privés profitent de cette vulnérabilité pour proposer des solutions qui sont trop dispendieuses, qui ne répondent pas aux besoins identifiés, etc.

Les acteurs privés pourraient d'ailleurs profiter de cette vulnérabilité pour proposer des outils qui ne sont pas suffisamment flexibles, c'est-à-dire qui peuvent être utilisés uniquement dans quelques contextes précis, qui doivent recevoir fréquemment des mises à jour payantes, qui ne sont pas compatibles avec d'autres systèmes informatiques déjà en place, etc. Ce manque d'expertise interne des organismes publics peut également accroître de manière importante une relation de dépendance par rapport aux développeurs en matière d'intelligence artificielle et ainsi participer à diminuer leur autonomie.

Recommandation 10

Que le Gouvernement du Québec développe sa propre expertise interne en matière de développement en intelligence artificielle et de stockage de données, de manière à assurer son indépendance par rapport aux intérêts privés ou aux entreprises privées.

Conclusion

La reconnaissance faciale, tout comme l'intelligence artificielle, est un développement technologique important qui soulève plusieurs enjeux éthiques, entre autres portant sur la protection des libertés fondamentales et des droits fondamentaux des citoyens. Les contextes d'utilisation de la RF étant variés et divers, les membres de la CEST-Jeunesse ont privilégié une approche qui ne met pas une seule valeur ou un seul ensemble de valeurs qui aurait préséance dans l'ensemble des situations. Plutôt, les délibérations ont permis d'établir certaines priorités qui ont des implications au niveau de l'éthique : l'importance de l'égalité et de la non-discrimination ; l'exigence du consentement et la protection de l'autonomie de la personne ; l'éducation et la sensibilisation du public ; une recherche scientifique en matière de RF qui vise le bien commun ; l'imputabilité des acteurs ; et, finalement, l'indépendance des institutions publiques.

Plusieurs institutions et organismes pourraient être tentés d'utiliser un système de RF pour augmenter le sentiment de sécurité du public ou pour assurer une meilleure sécurité de celui-ci. Ceci pourrait en effet être un bénéfice majeur lié à l'utilisation de la RF, surtout en ce qui concerne la sécurité des individus les plus vulnérables de la société. Les membres de la CEST-Jeunesse considèrent toutefois que l'utilisation de la RF à des fins de sécurité doit être encadrée de manière importante et qu'il faut éviter les dérives sécuritaires. La recommandation 3 vise à encadrer l'utilisation de la RF à des fins de sécurité. Un tel encadrement pourrait aussi participer de façon importante à mettre de l'avant l'égalité de tous les citoyens et l'exigence de non-discrimination. La recommandation 5, en portant sur les cas où il pourrait y avoir un préjudice possible, cherche aussi à donner les outils essentiels pour que le droit à la non-discrimination soit respecté.

La sensibilisation du public et l'importance de pouvoir consentir librement à l'utilisation de la RF ont grandement retenu l'attention des membres de la CEST-Jeunesse lors des délibérations. C'est dans ce contexte que s'inscrivent les recommandations 1, 2 et 4 : elles visent à implanter les conditions optimales pour que les citoyens puissent offrir un consentement valide à l'utilisation de la RF.

La CEST-Jeunesse considère qu'il est du devoir du Gouvernement du Québec de veiller à sensibiliser et éduquer le public. Celui-ci a aussi la responsabilité d'assurer que les différents acteurs liés au développement de la RF et de l'IA demeurent imputables. Les recommandations 6, 7 et 8 étayaient la manière dont les membres de la CEST-Jeunesse considèrent que, minimalement, le Gouvernement doit agir pour assurer cette imputabilité.

Les membres de la CEST-Jeunesse considèrent aussi que les bénéfices liés à la recherche en RF et en IA financée par les organismes gouvernementaux ne peuvent être que privés. La recommandation 9 souligne donc l'importance que ce financement soit au bénéfice de l'ensemble de la collectivité. Finalement, le Gouvernement du Québec devrait aussi chercher à développer sa propre expertise en matière d'IA, entre autres pour assurer son indépendance par rapport aux entreprises privées. C'est l'objectif visé par la recommandation 10 proposée par les membres de la CEST-Jeunesse.

Toutes ces recommandations sont audacieuses, mais nécessaires pour que le développement de la reconnaissance faciale favorise le bien commun.

Médiagraphie

AGENCE FRANCE PRESSE (2019). « Nice va tester la reconnaissance faciale sur la voie publique », *Le Monde*, 18 février 2019, https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html (consulté le 10 juillet 2019)

AMAZON REKOGNITION (S.D.). « Faits concernant la reconnaissance faciale avec l'intelligence artificielle », *Amazon*, <https://aws.amazon.com/fr/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/> (consulté le 19 juillet 2019).

ARCANGEL, A. (2018). « Snapchat Filters : How Do They Work ? », *Dev*, 31 janvier 2018, [En ligne] <https://dev.to/aubreyarcangel/snapchat-filters-how-do-theywork-4c83> (consulté le 29 janvier 2020).

BROWNEE, J. (2019). « A Gentle Introduction to Computer Vision », *Machine Learning Mastery*, 19 mars 2019, [En ligne] <https://machinelearningmastery.com/what-is-computer-vision/> (consulté le 27 février 2020).

CARABANTES, M. (2019). « Black-Box Artificial Intelligence : An Epistemological and Critical Analysis », *AI & Society*, [En ligne] <https://doi.org/10.1007/s00146-019-00888-w> (consulté le 30 janvier 2020).

CBINSIGHTS (2019). « Like It Or Not Facial Recognition Is Already Here. These Are The Industries It Will Transform First », *CBInsight*, 10 avril 2019, [En ligne] <https://www.cbinsights.com/research/facial-recognition-disrupting-industries/> (consulté le 29 janvier 2020).

CHARTRE CANADIENNE DES DROITS ET LIBERTÉS, PARTIE I DE LA LOI CONSTITUTIONNELLE DE 1982 : À JOUR AU 1^{er} MAI 2020, [Canada], [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.)], Gouvernement du Canada.

CHARTRE DES DROITS ET LIBERTÉ DE LA PERSONNE (RLRQ), C. C-12 : À JOUR AU 1^{er} FÉVRIER 2020, [Québec], Éditeur officiel du Québec.

CNIL (2019). « Reconnaissance faciale. Pour un débat à la hauteur des enjeux », CNIL, 15 novembre 2019, [En ligne] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf (consulté le 30 janvier 2020).

CODE CRIMINEL (LRC), C. C-46 : À JOUR AU 21 AVRIL 2020. [Canada], Gouvernement du Canada.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA (2013). « Reconnaissance faciale automatisée dans les secteurs public et privé », *Gatineau*, mars 2013, [En ligne] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/ (consulté le 6 août 2019).

COMMISSION D'ACCÈS À L'INFORMATION (2016). « Rétablir l'équilibre. Rapport quinquennal 2016 », Gouvernement du Québec.

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2005). « L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques », Gouvernement du Québec.

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2008). « Viser un juste équilibre : un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité », Gouvernement du Québec.

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2016). « Enjeux éthiques liés au *trading* haute fréquence », Gouvernement du Québec.

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2017A). « Reconnaissance faciale dans les aéroports : Qu'est-ce qu'elle a ma gueule ? », *Éthique hebdo*, 10 mars 2017, <https://www.facebook.com/notes/commission-de-lethique-en-science-et-en-technologie/ethique-hebdo-du-10-mars-2017-reconnaissance-faciale-dans-les-aeroports-quest-ce/1406035206105404/> (consulté le 15 juillet 2019).

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2017B). « La ville intelligente au service du bien commun : lignes directrices pour allier l'éthique au numérique dans les municipalités au Québec », Gouvernement du Québec.

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE (2018). « Éthique et cybersociété : un regard posé par des jeunes », *Avis de la CEST-Jeunesse* 2018, Gouvernement du Québec.

CHAMPAGNE, S. R. (2018A). « Trois questions sur la vie privée au philosophe Jocelyn Maclure », *Le Devoir*, 17 mars 2018, [En ligne] <https://www.ledevoir.com/societe/science/522941/trois-questions-au-philosophe-jocelyn-maclure> (consulté le 30 janvier 2020).

CHAMPAGNE, S. R. (2018B). « Reproduire les réactions faciales au cinéma », *Le Devoir*, 17 mars 2018, [En ligne] <https://www.ledevoir.com/societe/science/522944/le-clonage-des-reactions-faciales> (consulté le 30 janvier 2020).

COUTURE, P. (2019). « Reconnaissance faciale : les consommateurs épiés à leur insu dans les commerces », *Journal de Québec*, 11 mai 2019, [En ligne] <https://www.journaldequebec.com/2019/05/11/souriez-on-vous-surveille-par-la-reconnaissance-faciale> (consulté le 8 juillet 2019).

CUTHBERTSON, A. (2018). « Indian police trace 3,000 missing children in just four days using facial recognition technology », *Independent*, 24 avril 2018, [En ligne] <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html> (consulté le 30 janvier 2020).

DAVIS WEST, J. (2017). « A Brief History of Face Recognition », *FaceFirst*, 1^{er} août 2017, [En ligne] <https://www.facefirst.com/blog/brief-history-of-face-recognition-software/> (consulté le 30 janvier 2020).

DÉCLARATION DE MONTRÉAL (2018). « La déclaration de Montréal pour un développement responsable de l'intelligence artificielle », Université de Montréal, [En ligne] <https://www.declarationmontreal-iaresponsable.com/la-declaration> (consulté le 6 août 2019).

DODDS, L. (2018). « Chinese businesswoman accused of jaywalking after AI camera spots her face on an advert », *The Telegraph*, 25 novembre 2018, [En ligne] <https://www.telegraph.co.uk/technology/2018/11/25/chinese-businesswoman-accused-jaywalking-ai-camera-spots-face/> (consulté le 30 janvier 2020).

GEITGEY, A. (2016). « Machine Learning is Fun ! Part 4 : Modern Face Recognition with Deep Learning », *Medium*, 24 juillet 2016, [En ligne] <https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cfc121d78> (consulté le 7 août 2019).

GEMALTO (2020). « Facial recognition : top 7 trends (tech, vendors, markets, use cases and latest news) », *Gemalto*, 22 janvier 2020, [En ligne] <https://www.gemalto.com/govt/biometrics/facial-recognition> (consulté le 29 janvier 2020).

GIEC (2018). « Summary for Policymakers », *Global Warming of 1.5°C. An IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty* [Masson-Delmotte, V., P. Zhai, H.-O. Pörtner, D. Roberts, J. Skea, P.R. Shukla, A. Pirani, W. Moufouma-Okia, C. Péan, R. Pidcock, S. Connors, J.B.R. Matthews, Y. Chen, X. Zhou, M.I. Gomis, E. Lonnoy, T. Maycock, M. Tignor, and T. Waterfield (dir.)]. World Meteorological Organization, Genève, Suisse, 32 p.

GOSEPATH, S. (2007). « Equality », *Stanford Encyclopedia of Philosophy*, [En ligne] <https://plato.stanford.edu/entries/equality/> (consulté le 25 avril 2020).

GROTHER, P. ET AL. (2019). « Face Recognition Vendor Test (FRVT) – Part 3 : Demographic Effects », *National Institute of Standards and Technology*, [En ligne] <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (consulté le 30 janvier 2020).

HAO K. (2019). « AI researchers need to stop hiding the climate toll of their work », *MIT Technology Review*, 2 août 2019, [En ligne] <https://www.technologyreview.com/2019/08/02/102832/ai-research-has-an-environment-climate-toll/> (consulté le 30 janvier 2020).

HARWELL, D. ET A. BHATTARA (2018). « Inside Amazon Go : The camera-filled convenience store that watches you back », *The Washington Post*, 22 janvier 2018, [En ligne] <https://www.washingtonpost.com/news/business/wp/2018/01/22/inside-amazon-go-the-camera-filled-convenience-store-that-watches-you-back/> (consulté le 27 avril 2020).

HARWELL, D. (2019). « A face-scanning algorithm increasingly decides whether you deserve the job », *The Washington Post*, 6 novembre 2019, [En ligne] <https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/> (consulté le 26 février 2020).

HERMANN, V. (2017). « Face ID : sécurité, fonctionnement et limites de la reconnaissance faciale d'Apple », *Next Impact*, 28 septembre 2017, [En ligne] <https://www.nextinpact.com/news/105286-face-id-securite-fonctionnement-et-limites-reconnaissance-faciale-dapple.htm> (consulté le 19 juillet 2019).

HOOK, K. (2013). « Affective Computing », dans Lowgren Jonas et al., *The Encyclopedia of Human-Computer Interaction*, 2nd Ed., Interaction Design Foundation, [En ligne], <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/affective-computing> (consulté le 27 février 2020).

LAROUSSE (S.D.). « BASE DE DONNÉES », [En ligne], https://www.larousse.fr/encyclopedie/divers/base_de_donn%C3%A9es/185906 (consulté le 7 juillet 2019).

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ (RLRQ), C. P-39.1 : À JOUR AU 1^{er} FÉVRIER 2020, [Québec], Éditeur officiel du Québec.

LOI SUR LE DÉVELOPPEMENT DURABLE (RLRQ), C. D-8.1.1 : À JOUR AU 1^{er} FÉVRIER 2020, [Québec], Éditeur officiel du Québec.

LU D. (2019). « Creating an AI can be five times worse for the planet than a car », *New Scientist*, 6 juin 2019, [En ligne] <https://www.newscientist.com/article/2205779-creating-an-ai-can-be-five-times-worse-for-the-planet-than-a-car/> (consulté le 27 février 2020).

LUO, M. (2018). « Google Arts & Culture », *Google*, 17 janvier 2018, [En ligne] <https://www.blog.google/outreach-initiatives/arts-culture/exploring-art-through-selfies-google-arts-culture/> (consulté le 30 janvier 2020).

MASSOUD, R. (2018). « Militarisation de l'intelligence artificielle : "L'ampleur des dégâts pourrait être sans limites" », *ICI Radio-Canada*, 5 avril 2018, [En ligne] <https://ici.radio-canada.ca/nouvelle/1093360/google-maven-intelligence-artificielle-technologie-pentagone-wendell-wallach-yale-militarisation> (consulté le 30 janvier 2020).

MICROSOFT AZURE, « Face. An AI service that analyzes faces in images », [En ligne] <https://azure.microsoft.com/en-us/services/cognitive-services/face/> (consulté le 30 janvier 2020).

MINISTÈRE DE L'ÉCONOMIE ET DE L'INNOVATION (2020). « Les investissements en intelligence artificielle », [en ligne] <https://www.economie.gouv.qc.ca/bibliotheques/secteurs/technologies-de-linformation-et-des-communications/intelligence-artificielle/les-investissements-en-intelligence-artificielle/> (consulté le 10 février 2020).

MOZUR, P. (2019). « One Month, 500,000 Face Scans : How China Is Using A.I. to Profile a Minority », *New York Times*, 14 avril 2019, [En ligne] <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>, (consulté le 15 juillet 2019).

NDTV (2018). « FACIAL RECOGNITION SYSTEM HELPS TRACE 3,000 MISSING CHILDREN IN 4 DAYS », [En ligne] <https://www.ndtv.com/india-news/facial-recognition-system-helps-trace-3-000-missing-children-in-4-days-1841192> (consulté le 18 mars 2020).

NISSENBAUM, H. (2001). « How computer systems embody values », *Computer*, vol. 34, n°3, mars 2001, p.118-120.

OMS (1998). *Sécurité et promotion de la sécurité : Aspect conceptuels et opérationnels*, [En ligne] https://www.inspq.qc.ca/pdf/publications/149_SecuritePromotion.pdf (consulté le 26 février 2020).

PÉGNY, M. ET IBNOUHSEIN, I. (2018). « Quelle transparence pour les algorithmes d'apprentissage machine ? », [En ligne] https://www.researchgate.net/publication/331145970_Quelle_transparence_pour_les_algorithmes_d'apprentissage_machine (Consulté le 7 août 2019).

RADIO-CANADA (2018). « Il faut rendre la possession de robots tueurs immorale, estime Yoshua Bengio », *ICI Radio-Canada*, 19 novembre 2019, [En ligne] <https://ici.radio-canada.ca/nouvelle/1136739/yoshua-bengio-robots-tueurs-intelligence-artificielle-militaire-collaboration-internationale-recherche-apprentissage-profond> (consulté le 30 janvier 2020).

SMITH, M. J., CARAYON, P., SANDERS, K. J., LIM, S-Y. ET LEGRANDE, D. (1992). « Employee stress and health complaints in jobs with and without electronic performance monitoring », *Applied Ergonomics*, vol. 23, n°1 (février 1992), p. 17-27.

STATISTIQUE CANADA (2017). « Les statistiques : le pouvoir des données ! Glossaire », *Gouvernement du Canada*, [En ligne] <https://www150.statcan.gc.ca/n1/edu/power-pouvoir/glossary-glossaire/5214842-fra.htm#b> (consulté le 7 août 2019).

SUBASIC, E., REYNOLDS, K. J., TURNER, J. C., VEENSTRA, K. E. ET HASLAM, A. (2011). « Leadership, power and the use of surveillance : Implications of shared identity for leaders' capacity to influence », *The Leadership Quarterly*, vol. 22, n°1 (février 2011), p. 170-181.

THE MEDICAL FUTURIST (2019). « Your Guide to Facial Recognition Technology in Healthcare », *The Medical Futurist*, 19 novembre 2019, [En ligne] <https://medicalfuturist.com/your-guide-to-facial-recognition-technology-in-healthcare/> (consulté le 29 janvier 2020).

TILLMAN, M.(2019). « What are Memoji ? How to create an Animoji that looks like you », *Pocket-lint*, 18 septembre 2019, [En ligne] <https://www.pocket-lint.com/phones/news/apple/144743-what-are-memoji-how-to-create-an-animoji-that-looks-like-you> (consulté le 29 janvier 2020).

TOKYO 2020 (2020). « Face Recognition to be Pioneered at Olympic and Paralympic Games Tokyo 2020 », *Tokyo 2020*, [En ligne] <https://tokyo2020.org/en/news/notice/20180807-03.html> (consulté le 30 janvier 2020).

WEISS, E. (2019) « Camatica Uses Mood Analytics to Track Employee Satisfaction », *Find Biometrics*, 29 juillet 2019, [En ligne] <https://findbiometrics.com/camatica-uses-mood-analytics-track-employee-satisfaction-072903/> (consulté le 26 février 2020).

ZHAO, Y. ET AL. (2018). « A Face Recognition Application for People with Visual Impairments : Understanding Use Beyond the Lab », *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems – CHI '18*, Montreal, ACM Press, p. 1-14.

Glossaire

ALGORITHME

Une méthode de résolution de problèmes par une suite finie et non ambiguë d'opérations. Plus précisément dans le domaine de l'intelligence artificielle, il s'agit de la suite d'opérations appliquées aux données d'entrée pour arriver au résultat désiré. (Déclaration de Montréal, 2018.)

APPRENTISSAGE MACHINE (MACHINE LEARNING)

L'apprentissage machine est la branche de l'intelligence artificielle qui consiste à programmer un algorithme à apprendre par lui-même. Parmi la multitude de techniques, on distingue trois types majeurs d'apprentissage machine :

1. En apprentissage supervisé, le système d'intelligence artificielle (SIA) apprend à prédire une valeur à partir d'une donnée entrée. Cela nécessite d'avoir des couples entrée-valeur annotés lors de l'entraînement. Par exemple, un système peut apprendre à reconnaître l'objet présent sur une photo ;
2. En apprentissage non supervisé, le SIA apprend à trouver des similitudes entre des données qui n'ont pas été annotées, par exemple afin de les diviser en différentes partitions homogènes. Ainsi, un système peut reconnaître des communautés d'utilisateurs de réseaux sociaux ;
3. En apprentissage par renforcement, le SIA apprend à agir sur son environnement de façon à maximiser une récompense qui lui est donnée lors de l'entraînement. C'est la technique avec laquelle des SIA ont pu battre des humains au jeu de Go ou au jeu vidéo Dota2. (Déclaration de Montréal, 2018.)

APPRENTISSAGE PROFOND (DEEP LEARNING)

L'apprentissage profond est la branche de l'apprentissage machine qui utilise des réseaux de neurones artificiels à plusieurs niveaux. C'est la technologie qui est derrière les plus récentes avancées en IA. (Déclaration de Montréal, 2018.)

ASSOCIATION (DES VISAGES)

Comparaison du visage à partir d'une photo ou d'une vidéo avec une base de données afin de découvrir ou de confirmer l'identité d'un individu.

AUTHENTIFICATION (À PARTIR DU VISAGE)

Autorisation à accéder à une ressource (ex. appareil électronique ou lieu physique, comme un iPhone ou une salle sécurisée) par un système de reconnaissance faciale qui permet de valider l'identité du demandeur d'accès à la ressource.

BASE (OU BANQUE) DE DONNÉES

Ensemble structuré de fichiers regroupant des informations ayant certains caractères en commun ; logiciel permettant de constituer et de gérer ces fichiers. (Larousse, s. d.)

BIAIS ALGORITHMIQUE

Dans l'estimation de la valeur d'un paramètre d'une répartition de probabilités, c'est la différence entre la valeur prévue et la valeur réelle du paramètre (Statistique Canada, 2017). Un biais peut aussi être une erreur dans le résultat, pouvant par exemple provenir d'une mauvaise qualité ou représentativité des données utilisées pour entraîner et programmer les algorithmes.

BIOMÉTRIE

Un système biométrique permet d'identifier une personne ou de vérifier l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche) ». (CEST, 2008.)

DÉTECTION DE VISAGES

La détection des visages, qui consiste à trouver un visage dans une image, est moins précise que la reconnaissance faciale. On n'établit aucune correspondance avec l'image d'un individu identifié. (Commissariat à la protection de la vie privée au Canada, 2013.)

DONNÉES PERSONNELLES

Les données personnelles sont celles qui permettent d'identifier directement ou indirectement un individu. (Déclaration de Montréal, 2018.)

Aussi : données à caractère personnel, renseignements personnels.

EMPREINTE FACIALE (FACEPRINT)

Cartographie d'un visage réalisée par un algorithme à partir d'une photo ou d'une vidéo en détectant plusieurs dizaines de points de repère (*landmarks*) qui sont communs à tous les visages.

ENTRAÎNEMENT

L'entraînement est le processus de l'apprentissage machine pendant lequel le [système d'intelligence artificielle] SIA construit un modèle à partir de données. Les performances du SIA dépendront de la qualité du modèle, lui-même dépendant de la quantité et de la qualité des données utilisées durant l'entraînement. (Déclaration de Montréal, 2018.)

FAUX POSITIF / FAUX NÉGATIF

Un faux positif est un résultat déclaré positif par un système alors qu'il est négatif dans les faits. Un faux négatif est l'inverse. Peut se mesurer en « taux » afin d'évaluer l'efficacité d'un système de reconnaissance faciale.

FIABILITÉ

Un système d'IA est fiable lorsqu'il effectue la tâche pour laquelle il a été conçu de manière attendue. La fiabilité est la probabilité de succès qui varie entre 51 % et 100 %, c'est-à-dire qui est strictement supérieur au hasard. Plus un système est fiable, plus son comportement est prévisible. (Déclaration de Montréal, 2018.)

IDENTIFICATION (DU VISAGE)

Établissement de l'identité d'un individu à partir de son visage sur une photo ou une vidéo.

INTELLIGENCE ARTIFICIELLE (IA)

L'intelligence artificielle (IA) désigne l'ensemble des techniques qui permettent à une machine de simuler l'intelligence humaine, notamment pour apprendre, prédire, prendre des décisions et percevoir le monde environnant. Dans le cas d'un système informatique, l'intelligence artificielle est appliquée à des données numériques. (Déclaration de Montréal, 2018.)

INTELLIGIBILITÉ

Un système d'IA est intelligible lorsqu'un être humain doté des connaissances nécessaires peut comprendre son fonctionnement, c'est-à-dire son modèle mathématique et les processus qui le déterminent. (Déclaration de Montréal, 2018.)

JEU DE DONNÉES NUMÉRIQUES (DATASET)

Agrégation de données organisées en un ensemble cohérent qui peut être analysé par traitement informatique. Cette collection de données représente un ensemble au sein d'une base ou banque de données.

RECONNAISSANCE FACIALE (RF)

La reconnaissance faciale (RF) est une technologie qui utilise des algorithmes d'intelligence artificielle (IA) pour identifier un individu sur une image ou dans une vidéo. L'utilisation classique de la RF est à des fins d'identification ou de confirmation de l'identité d'une personne avec une ou plusieurs de ses caractéristiques biologiques. C'est en ce sens que la RF fait partie de la classe plus large des systèmes biométriques, qui permettent d'identifier les individus grâce à leurs caractéristiques propres : empreinte digitale, iris de l'œil, traits du visage, etc. La RF peut aussi être utilisée pour analyser les caractéristiques d'un individu, dont son âge, son genre, ses émotions, sans nécessairement chercher à identifier celui-ci.

Annexe 1

Description de l'activité CEST-Jeunesse 2019-2020

La CEST-Jeunesse est une activité de la Commission de l'éthique en science et en technologie destinée aux étudiants de niveau collégial. Elle se tient tous les deux ans. Elle est constituée d'une quinzaine d'étudiants provenant de diverses régions du Québec, qui sont sensibilisés à l'éthique par l'analyse d'un thème choisi par la CEST et préparent un avis sur la question. Cet avis est entériné et publié par la CEST. Les avis et les outils de sensibilisation découlant de ces éditions sont disponibles sur le site de la CEST (www.ethique.gouv.qc.ca).

La CEST-Jeunesse 2020 a porté sur les enjeux soulevés par les technologies de reconnaissance faciale et s'est réunie du 13 au 16 janvier 2020. Le travail préparatoire aux journées de délibération a été réalisé lors de la session d'automne 2019 dans les quatre cégeps participants (Cégep André-Laurendeau, Cégep de la Gaspésie et des Îles, Collège Jean-de-Brébeuf et Cégep de Sainte-Foy), et ce, sous la supervision d'enseignants de philosophie.

Les visées pédagogiques

- S'approprier un thème donné afin d'en déterminer les enjeux éthiques ;
- Pratiquer la délibération éthique sur les différentes facettes du thème à l'étude, avec pour objectif la détermination et la hiérarchisation (ou « priorisation ») des valeurs en jeu ;
- Savoir formuler des recommandations destinées aux décideurs politiques, institutionnels et aux autres interlocuteurs que le sujet peut concerner.

Les objectifs

La CEST-Jeunesse 2020 a pour mandat de réfléchir aux enjeux soulevés par l'utilisation de technologies de reconnaissance faciale, ainsi que de formuler des recommandations en réponse à ces enjeux. Ces recommandations seront portées à l'attention de la Commission de l'éthique en science et en technologie, qui pourra les commenter et, si elle le juge pertinent, les adresser officiellement aux destinataires appropriés. Leur diffusion enrichira le débat public en relayant la perspective de jeunes étudiants.

Plus précisément, les objectifs poursuivis lors de la 8^e édition sont les suivants :

- Recueillir et transmettre une information claire et juste sur le sujet à l'étude ;
- Circonscrire les caractéristiques pertinentes à l'analyse éthique, en déterminant les valeurs en jeu et les conséquences sur les personnes, groupes ou organisations concernés ;
- Formuler, à l'attention des décideurs politiques ou institutionnels et des autres interlocuteurs que le sujet peut concerner, des recommandations pour faire face aux enjeux éthiques soulevés par l'utilisation de technologies de reconnaissance faciale. Ces recommandations sont soutenues par un argumentaire éthique qui suscite le consensus parmi les membres de la CEST-Jeunesse ;
- Produire un rapport clair, concis et rigoureux, fidèle aux conclusions obtenues à l'issue des journées de délibération.

Annexe 2

Programme des journées de travail de la CEST-Jeunesse 2019-2020

Lundi 13 janvier 2020

13 h Accueil des participant(e)(s)
• **M. Jocelyn Maclure**, président de la CEST

13 h 30 Présentation des participant(e)(s)
Présentation des experts-conseil
• **M. Pierre-Luc Déziel**, professeur à la Faculté de droit de l'Université Laval et spécialiste du droit à la vie privée dans le contexte numérique
• **M^{me} Sarah Gagnon-Turcotte**, conseillère en stratégie et innovation, chargée de projet chez Nord Ouvert
• **M. Martin Gibert**, chercheur au Centre de recherche en éthique et à l'Institut de valorisation des données et spécialiste de l'éthique de l'intelligence artificielle et de la psychologie morale

Présentation de l'animatrice
• **M^{me} Manon Lortie**, enseignante en philosophie au CÉGEF de Jonquière et ambassadrice émérite de la CEST-Jeunesse

14 h 30 Première séance de travail
Objectifs : Synthétiser les travaux réalisés dans chacun des cégeps, procéder à une première mise en commun des réflexions

17 h Fin de la première séance de travail

Mardi 14 janvier 2020

9 h Séance de travail
Objectif : Retour en commun sur les discussions de la journée précédente pour faire ressortir les valeurs et principes en jeu avant d'aborder les mises en situation

11 h 30 Synthèse des échanges / questions ou commentaires des observateurs

12 h Dîner

13 h 15 Séance de travail
Objectif : Travailler sur les mises en situation : définir les termes, identifier les dilemmes ou enjeux éthiques et identifier des pistes de solution

16 h 30 Synthèse des échanges / questions ou commentaires des observateurs

17 h Fin de la journée de travail

Mercredi 15 janvier 2020

9 h Séance de travail
Objectifs : Retour sur les mises en situation et les enjeux qui y sont soulevés, atteindre un consensus sur l'analyse des enjeux

11 h 30 Synthèse des échanges / questions ou commentaires des observateurs

12 h Dîner

13 h 15 Séance de travail
Objectif : Développer l'argumentaire à mettre de l'avant dans l'avis

16 h 30 Synthèse des échanges / questions ou commentaires des observateurs
Nomination des porte-paroles officiels de la CEST-Jeunesse 2020

17 h Fin de la journée de travail

Jeudi 16 janvier 2020

9 h Séance de travail
Objectif : Finaliser l'argumentaire et établir les éléments à mettre de l'avant de manière prioritaire dans la communication des conclusions des délibérations

11 h Questions ou commentaires des observateurs

11 h 45 Synthèse finale et mots de remerciements du président

12 h Dîner

Clôture de la CEST-Jeunesse 2020

*Commission
de l'éthique
en science
et en technologie*

Québec 