HEC MONTRÉAL

Étude exploratoire sur les enjeux éthiques reliés à l'informatique affective et la gestion des données personnelles

par

Frédérique Godin
11255705

Science de la Gestion
(Option Développement Organisationnel)

Projet supervisé présenté en vue de l'obtention
du grade de maîtrise ès sciences
(M. Sc.)

Décembre 2020

RÉSUMÉ

Ce rapport de projet supervisé explore les enjeux éthiques reliés à l'informatique affective et la gestion des données personnelles. Il comprend également une analyse stratégique de l'environnement externe d'EmoSciens, une *startup* québécoise utilisant la technologie de l'informatique affective, ainsi qu'un *benchmark* au niveau éthique. Ces deux composantes du rapport permettront à cette jeune entreprise d'avoir une vue d'ensemble des différents éléments avec lesquels elle devra composer alors que son écosystème est en évolution rapide.

Le projet arrive à un moment opportun pour la *startup*. Effectivement, alors que les technologies d'intelligence artificielle ne font que prendre de l'ampleur sur le marché, la méfiance qu'elles génèrent menace leur acceptation sociale. Les enjeux éthiques présentés dans ce présent rapport sont ceux qui doivent être exposés et traités si l'industrie et la société espèrent se développer de façon responsable.

MOTS CLÉS

Big Data; intelligence artificielle; informatique affective; enjeux éthiques; données personnelles

TABLE DES MATIÈRES

LISTES DES TABLEAUX ET FIGURES

LISTE DES ABRÉVIATIONS

RGPD: Règlement général sur la protection des données

CCPA: *California Consumer Privacy Act*

FTC: *Federal Trade Commission*

INAD : Interface neuronale affective directe

UE : Union européenne

IA : Intelligence artificielle

CIFAR : *Canadian Institute for Advanced Research* (Institut canadien de recherches avancées)

TAC : Technologies améliorant la confidentialité

OCDE : Organisation de coopération et de développement économique

REMERCIEMENTS

Ce projet représente la fin d'un long chapitre et le tremplin vers un second que j'aborde avec le plus grand enthousiasme. Le rapport qui en découle est l'expression écrite et concrète de nombreux efforts que je n'aurais pu déployer sans l'aide et le support de plusieurs personnes que je tiens à souligner ici.

D'abord, merci à Joé T. Martineau, non seulement pour m'avoir pris sous ta direction, mais aussi pour l'inspiration que ta personne et ton enseignement ont représentée pour moi. Merci de m'avoir accompagné avec toute ton humanité dans l'incertitude et la découverte du domaine de l'éthique de l'intelligence artificielle. Ton apport dans mon cheminement académique et bientôt professionnel se fera sentir longtemps.

J'aimerais remercier Pierrich Plusquellec et l'équipe d'EmoScienS de m'avoir rencontré dans mes aspirations personnelles et professionnelles en me fournissant un terrain fertile à défricher. Merci pour cette expérience formatrice et cette confiance, malgré l'inexpérience, qui m'ont permis de m'immerger dans un vaste univers qui m'était encore largement inconnu. Ce projet représente un moment décisif pour moi. Il représente la validation d'un intérêt nouveau et insoupçonné, ainsi que le premier pas dans une direction qui, pour une fois, me stimule réellement.

Je tiens à remercier mon ami Santiago, celui qui a prononcé les mots « éthique de l'intelligence artificielle » de façon banale sans se douter qu'une petite conversation de coin de table serait autant bénéfique pour moi. Cette dernière aura été le déclic incroyablement bien placé dont j'avais besoin pour trouver ma direction. C'est à partir de ce moment que j'ai enfin su où je m'en allais, et pour cela, je te remercie du fond du cœur.

J'aimerais finalement remercier certains professeurs marquants qui, à travers leur enseignement et leur approche profondément humaine, m'ont aidé à faire des pas de géants dans ma quête personnelle. C'est incroyable à quel point certains d'entre eux m'ont appris, au-delà des théories, à embrasser de façon authentique la personne que je deviens. Merci pour tout.

INTRODUCTION

L'intelligence artificielle pour qui? De prime abord, l'automatisation de tâches et de services habituellement effectués par des êtres humains faillibles et imparfaits semble bénéficier le grand public plus que quiconque. Ce n'est qu'à la vue de scandales de fuite de données à la Desjardins (Desjardins, 2019), de discrimination algorithmique à la COMPAS rapportée par ProPublica (Angwin, Larson, Mattu et Kirchner, 2016) et de manipulation d'opinions de masse à la Cambridge Analytica (Cadwalladr et Graham-Harrison, 2018) que la réponse n'est plus si claire.

Les avancées que connaissent l'intelligence artificielle et l'industrie du Big Data sont à la fois fascinantes et terrifiantes. C'est ce que le pouls de la société nous révèle. Ces technologies possèdent une dualité inhérente qui les rend capables du meilleur et du pire. Si leur présence dans la vie de plusieurs est gage d'efficacité, de rapidité et de facilité, leur passage dans celle d'autres laisse des marques parfois indélébiles qui font ressurgir les maux de notre société. Effectivement, la délégation de plusieurs fonctions jusqu'à tout récemment humaines à des systèmes d'intelligence artificielle peut causer des dommages imprévus et créer des situations d'injustice qui remettent en cause certains supposés bénéfices de ces technologies.

Qui plus est, ces technologies se développent à une vitesse fulgurante. Le manque de régulation et l'absence de cadres législatifs pour encadrer leur développement et leur utilisation transforment le marché des technologies en un terrain de jeu sans règles ni contraintes pour les grandes corporations. Ce contexte s'avère particulièrement propice aux abus de confiance et de pouvoir qui nous font remettre en question la place de l'utilisateur dans l'industrie. Effectivement, ces technologies servent parfois des fins qui ne bénéficient qu'une minorité et qui entravent le bien-être de la société.

Cette situation a suscité la mobilisation d'acteurs internationaux autour de la question de l'éthique de l'intelligence artificielle et du Big Data dans les dernières années. Effectivement, alors que l'éthique nous pousse à nous questionner sur les valeurs qui dirigent nos comportements et aux conséquences morales de ceux-ci, de nombreuses instances crédibles se sont dédiées à explorer

ces questions à travers des initiatives globales et la publication de guides et de rapports soulignant les dangers et implorant l'action. La déclaration de Montréal pour un développement responsable de l'IA publiée en 2018 en est un bon exemple. Avec ses dix principes éthiques, la déclaration vise à éclairer la voie à suivre pour le développement d'une l'IA responsable, faciliter la transition numérique et ouvrir le dialogue international sur la question. Malgré tout, certaines critiques demeurent. Certains reprochent à ces initiatives de manquer d'applicabilité et tardent à porter leurs fruits. Comment opérationnaliser toutes ces valeurs et les traduire en pratiques concrètes? Et surtout, saurons-nous le faire à temps? Les besoins sont criants.

Le présent projet, en collaboration avec la jeune *startup* montréalaise EmoScienS, s'inscrit dans ce mouvement global du développement d'une IA responsable, pour le bien de tous. La motivation centrale de ce projet supervisé se résume par la question suivante : comment bénéficier de tout le potentiel de l'intelligence artificielle et du Big Data, sans compromettre la dignité humaine au passage? Le champ d'expertise de la *startup* en question nous poussera à nous immerger dans les domaines aux chevauchements multiples de l'éthique des données et de l'informatique affective. À travers cette exploration, nous soulèverons davantage d'enjeux que de solutions. Cependant, nous aborderons aussi des pistes de recommandations, et espérons que les bases érigées ici serviront d'assises solides à EmoScienS pour contribuer à un écosystème en plein changement de façon responsable et significative. Nous espérons que ce rapport contribuera, à sa façon, à faire avancer la cause d'une IA pour le bien de tous.

1. LE MANDAT

1.1 Présentation de l'entreprise partenaire

Le présent projet supervisé prend forme autour de besoins spécifiques formulés par la jeune *startup* EmoScienS qui offre un service propulsé par une technologie d'informatique affective. Cette technologie prend la forme d'une application qui, à l'aide d'algorithmes d'apprentissage profond, détecte les expressions faciales et reconnaît les émotions que ces expressions infèrent. Installée sur le téléphone ou l'ordinateur de l'utilisateur, l'application prend des photos du visage de ces derniers à intervalles réguliers. L'utilisation d'algorithmes de vision artificielle et d'apprentissage profond permet à l'application de capter les différents mouvements des muscles du visage et d'ensuite les associer aux six émotions que la technologie reconnaît.

La visée d'EmoScienS est d'offrir un produit/service à des clients individuels, mais sa portée est également organisationnelle. Effectivement, le client d'EmoScienS est l'organisation, mais son objectif principal est le développement de l'intelligence émotionnel des employés qui, quant à elle, peut avoir des retombées sur l'engagement et la performance de l'organisation. Pour ce faire, l'application que la *startup* propose offre un bilan émotionnel aux utilisateurs qui est généré sur une base hebdomadaire. À la fin de chaque semaine, les employés peuvent avoir une vue d'ensemble sur leur vécu émotionnel des jours précédents, présentée sous forme de graphiques, et prendre conscience des émotions qui ont dominé leur quotidien. Le bilan est présenté de pair avec du contenu éducatif sur les émotions pour augmenter la compréhension que les utilisateurs ont de leur vécu émotionnel. L'application propose également un système d'alerte de déviation du profil émotionnel personnalisé qui permet aux utilisateurs de prendre conscience de leurs fluctuations émotionnelles et prendre action. À cet effet, l'application d'EmoScienS prévoit différentes solutions selon le besoin. Dans un premier temps, l'application offre des exercices de régulation émotionnelle ciblés que les utilisateurs peuvent utiliser au moment où le besoin émerge. Pour les instances où les enjeux émotionnels des utilisateurs dépasseraient les capacités d'accompagnement et le support fournis par l'application, EmoScienS prévoit rediriger ceux-ci vers des ressources qui offrent des programmes validés par la science, comme des partenaires externes ou encore le programme d'aide aux employés de l'organisation cliente.

EmoScienS se veut une solution préventive à toutes les conséquences organisationnelles que peuvent engendrer les enjeux de régulation émotionnelle et de stress au travail. L'application d'EmoScienS s'avère un moyen concret et durable pour les organisations de bâtir une culture soucieuse du bien-être de leurs employés et d'améliorer leur performance globale.

Chez EmoScienS, l'éthique est le pilier du modèle d'affaires. Effectivement, l'équipe derrière la technologie est soucieuse d'offrir un service respectueux de la vie privée de ses utilisateurs et est désireuse de remettre le pouvoir entre les mains de ces derniers, ce qu'elle souligne sur son site internet par le passage suivant: « Parce que VOS données doivent d'abord et avant tout VOUS servir » (https://www.emosciens.com/). EmoScienS est animée par la conviction que les données émotionnelles des utilisateurs représentent un potentiel énorme pour ces derniers et elle se donne comme mandat premier d'exploiter ce créneau de façon responsable et éthique.

1.2 Présentation du mandat

Au moment d'écrire ces lignes, EmoScienS a déjà testé sa technologie pour la première fois auprès d'un petit échantillon d'adultes en contexte organisationnel et cherche à connaître les enjeux que celle-ci pourrait soulever pour améliorer sa proposition de valeur. Elle entame également un processus d'encadrement juridique et éthique pour la conception de sa politique de vie privée qui lui permettra d'ancrer l'éthique dans chacune de ses pratiques. Pour compléter sa démarche, EmoScienS a mandaté une étude exploratoire sur les enjeux éthiques reliés à l'informatique affective et la gestion des données personnelles. Plus spécifiquement, le mandat confié par la *startup* s'articule autour de deux axes qui vont comme suit :

Premier axe : revue de la littérature

Une revue de littérature portant sur les enjeux éthiques relatifs à la gestion des données personnelles et l'informatique affective. La revue de littérature fournira les connaissances nécessaires à l'équipe derrière la *startup* pour situer sa responsabilité face aux potentielles dérives et risques de la technologie qu'elle propose.

Deuxième axe : analyse de l'environnement externe

Une analyse PESTEL de l'environnement d'EmoScienS qui évalue l'état actuel de son écosystème ainsi que les éléments avec lesquels elle aura à composer dans un avenir proche.

Un *benchmark* qui permet de cibler les concurrents de la *startup* ainsi que de faire lumière sur les pratiques de gestion des données personnelles adoptées par l'industrie, permettant à cette dernière d'identifier les opportunités de positionnement concurrentiel dans son écosystème.

Une fois le mandat achevé, l'équipe derrière EmoScienS possédera des outils qui lui permettront de faire des choix responsables et éthiques. Le présent rapport permettra à EmoScienS de se situer dans un écosystème aux développements rapides à l'aide d'une technologie conçue dans le souci du bien-être de ses utilisateurs.

2. REVUE DE LITTÉRATURE

Nous sommes à l'ère du Big Data. À l'ère d'un Big Data omniprésent, omniscient et intrusif qui défie et parfois transcende la compréhension humaine. Ce phénomène relativement récent porte plusieurs définitions qui, teintées par différentes perspectives, ne reflètent qu'une infime partie d'une réalité très complexe et difficile à saisir. Comme le rapportent De Mauro, Greco et Grimaldi (2015) les principaux thèmes abordés par la littérature sur le Big Data concernent l'information qui lui sert de ressource, les technologies que l'exploitation des données massives nécessite, les méthodes qui lui permettent d'extraire la valeur des données et les impacts qu'elle a sur la société. Ces thèmes centraux sont reflétés dans les différentes définitions qui existent, mais ne se chevauchent que très rarement. Celle de Laney (2001, cité dans De Mauro, Greco et Grimaldi, 2015, traduction libre : 101) décrit le phénomène à l'aide de trois caractéristiques techniques, soit « Volume, Vélocité et Variété ». Cette définition reflète « la croissance explosive » du volume des données avec lesquelles l'industrie doit jongler, la rapidité avec laquelle les données sont « générées et transmises » ainsi que la diversité de sources et de formes que prennent les données collectées (Yang, Huang, Li, Liu et Hu, 2017, traduction libre : 14). Cette définition est fréquemment reprise et agrémentée au point où, alors que certains parlent de la définition des 3Vs, d'autres y ajoutent les termes « Véracité » et « Valeur » pour souligner « la diversité de qualité, d'exactitude et de fiabilité des données » ainsi que la précieuse utilité qu'elles ont pour ceux qui savent les mettre à profit (Yang, Huang, Li, Liu et Hu, 2017, traduction libre : 14; De Mauro, Greco et Grimaldi, 2015). Il devient alors parfois plus juste de parler de la définition des 4Vs ou encore des 5Vs (Marr, 2015, cité de Yang et al., 2017).

D'autres auteurs optent pour une définition qui reflète les nouvelles capacités requises pour l'exploitation des vastes quantités de données caractéristiques du Big Data (De Mauro, Greco et Grimaldi, 2015) comme Chen, Chiang et Storey (2012, traduction libre : 1166) qui définissent le phénomène comme étant « [un ensemble] de données et [de] techniques d'analyse d'applications qui sont si vastes et complexes qu'elles nécessitent des technologies avancées et uniques de stockage, de gestion, d'analyse et de visualisation des données ». Finalement, d'autres comme Boyd et Crawford (2012) définissent le Big Data comme un écosystème qui dépasse largement l'emblématique vastitude des banques de données que sous-entend son appellation. Effectivement,

les deux auteurs décrivent un « phénomène culturel, technologique et scientifique qui repose sur l'interaction entre la technologie, l'analytique et la mythologie » (Boyd et Crawford, 2012, traduction libre : 663).

Le Big Data est un outil de transformation puissant. Concrètement, il représente un exercice massif et continu de « datatification » des subtilités de la vie quotidienne en données lisibles et compréhensibles pour la machine (Cuckier et Mayer-Schoenberger, 2013, traduction libre : 29). L'analytique des données massives ouvre la porte sur une vaste étendue d'informations qui, jusqu'à tout récemment, étaient impossibles à toucher, en plus de permettre d'en dériver des connaissances et des conclusions qui portent désormais les seaux questionnables de la science et de l'objectivité (Cuckier et Mayer-Schoenberger, 2013; Boyd et Crawford, 2012; Zuboff, 2015; De Mauro, Greco et Grimaldi, 2015). Si les données dont il est question ici ne sont pas exclusivement personnelles et qu'elles n'offrent pas toutes le même regard intime sur la vie des gens, certaines le sont et beaucoup peuvent le devenir (Zwitter, 2014). Ces données personnelles, considérées comme le « pétrole de l'aire du numérique » (The world's most valuable resource, 2017, traduction libre), s'avèrent particulièrement lucratives. Effectivement, que ce soit à travers « l'amélioration de processus internes […], l'enrichissement des produits, des services et de l'expérience client [ou encore] la vente des données » (Wixom et Ross, 2017, traduction livre, p. 11), aucun prix ne semble trop cher payé pour s'emparer et bénéficier de données dont la valeur est inestimable. Le marché des technologies étant particulièrement féroce, la course à l'acquisition des banques de données donne naissance à des comportements organisationnels franchement douteux qui frôlent et parfois transgressent les limites de la moralité.

À la vue des pratiques néfastes qui parsèment l'industrie, certains comme Richards et King (2014, traduction libre : 395) appellent à la création d'une « éthique des données massives ». La littérature semble utiliser les termes « éthiques des données massives » et « éthique des données » de façon interchangeable et s'il n'est pas claire en quoi les deux diffèrent, mise à part leur échelle, Floridi et Taddeo (2016, traduction libre : 3) nous fournissent une définition détaillée et englobante de l'éthique des données qui semble convenir au phénomène des données massives :

> « L’éthique des données est la branche de l'éthique qui étudie et évalue les problèmes moraux liés aux données (y compris la génération, l'enregistrement, la conservation, le traitement, la diffusion, le partage et l'utilisation), aux algorithmes (y compris l'intelligence artificielle, les agents artificiels, l'apprentissage machine et les robots) et aux pratiques correspondantes (y compris l'innovation responsable, la programmation, le piratage et les codes professionnels), afin de formuler et de soutenir des solutions moralement bonnes (par exemple, les bonnes conduites ou les bonnes valeurs) ».

Comme le signalent les auteurs, cette définition illustre les « différentes dimensions morales des données » et souligne que les enjeux éthiques résident dans les manipulations qui sont faites des données, bien plus que dans les technologies qui les exploitent (Floridi et Taddeo, 2016, traduction libre : 3). Cette éthique permettrait d’établir les bases qui façonneront « [cette] nouvelle société du numérique [que] nous construisons », de sorte à ce qu’elle ne privilégie pas l’innovation et l’enrichissement au détriment des valeurs humaines qui nous sont chers (Richards et King, 2014, traduction libre : 395).

Maintenant, malgré que les technologies qui exploitent les données personnelles ne soient pas au cœur des enjeux que porte le phénomène des données massives, elles ne sont pas sans y contribuer. En vérité, les technologies d’intelligence artificielle, auxquelles le présent projet s’intéresse particulièrement, et le phénomène des données massives sont tout simplement indissociables. Effectivement, pour fonctionner l’intelligence artificielle nécessite un apport colossal en données souvent personnelles pour pouvoir entraîner les algorithmes qui sont derrière les différentes fonctionnalités que ses technologies offrent (Ostrom, Fotheringham et Bitner, 2019; Cockelbergh, 2020). Qui plus est, par l’exercice de leurs fonctions, ces technologies d’intelligence artificielle génèrent à leur tour des données personnelles qui contribuent à la croissance du phénomène des données massives (Cockelbergh, 2020). L’entreprise que nous accompagnons pour ce projet supervisé exploite une technologie d’intelligence artificielle issue d’un domaine émergent évoluant dans l'ombre depuis la fin des années 1990 qui présente un potentiel incroyable pour l'humanité, mais aussi des risques majeurs à prendre en considération : l'informatique affective. Originalement défini par Rosalind Picard (1995, traduction libre : 1) comme « l’informatique qui se rapporte à l'émotion, en découle ou l'influence », le domaine est actuellement restreint à quelques applications concrètes dont la majorité porte sur la détection, la reconnaissance et parfois

même la simulation des émotions. Par contre, la portée du domaine est beaucoup plus vaste. En effet, considérant l'importance des émotions dans la prise de décision, la littérature souligne l'importance de l'informatique affective dans la quête de rendre le robot toujours plus intelligent et adapté dans ses interactions avec l'humain, et dédie une partie de la réflexion à la possibilité d'un jour concevoir des robots munis d'émotions véritables (Richardson, 2017). Les données exploitées par les technologies d'informatique affective sont considérées comme « fondamentalement privées et personnelles » (Picard, 2003, traduction libre : 61), voire même sensibles (Steinert et Friedrich, 2020), cependant elles leur sont absolument essentielles pour fonctionner (Richardson, 2020). Ces données font donc partie de toutes celles qui flottent dans le nuage massif de données personnelles qu'exploite l'industrie du Big Data. Les risques sont non seulement nombreux, mais réels et imminents.

Avant d'introduire les différents enjeux qui composent la section qui suit, il nous faut faire un court détour supplémentaire pour aborder la question de la confiance. Pouvons-nous faire confiance au Big Data, à l'intelligence artificielle? Ou plutôt, devrions-nous ? La question est d'autant plus évidente lorsque l'on constate l'état des lieux dépeint par le rapport de Deloitte (2019) « Surmonter les risques, instaurer la confiance » qui reflète une méfiance et une incompréhension généralisées au sein de la population canadienne. Le gouvernement du Canada dédie même une charte entière à cette confiance, la charte canadienne du numérique, qui cite dix principes devant aider le gouvernement à « bâtir la confiance dans un monde numérique » (Innovation, Sciences et Développement Économique Canada, 2020). Pour sa part, l'OCDE en fait un point central dans sa démarche qui a mené à la Recommandation du Conseil sur l'intelligence artificielle adoptée le 22 mai 2019. Effectivement, alors que le mot confiance revient constamment à travers le document, l'organisation introduit ce dernier en mentionnant qu'il « vise à stimuler l'innovation et renforcer la confiance dans l'IA en promouvant une approche responsable au service d'une IA digne de confiance, tout en garantissant le respect des droits de l'homme et des valeurs démocratiques » (OCDE, 2020 : 3). L'espace qu'occupe l'enjeu de la confiance dans bon nombre d'initiatives globales souligne l'importance de s'y attarder rapidement, au risque de compromettre l'épanouissement d'une industrie qui, pour l'instant, ne s'attire que doute et méfiance.

La confiance se prouve, et ce, à plusieurs niveaux (Hand, 2018). Pour ce faire, « les organisations doivent remplir leurs obligations, se comporter de façon prévisible et ne pas se livrer à un comportement opportuniste inapproprié avec les données » personnelles des individus (Someh et al. 2019, traduction libre : 725), « tout en assurant [leur] sécurité » (Breidbach et al. 2019, traduction libre, 668). Est-ce que les géants du Big Data remplissent ces conditions? Comme nous le verrons, la revue de littérature qui suit présente une industrie opaque et coercitive qui donne raison aux sceptiques et justifie la prudence.

Les parties suivantes introduisent les différents enjeux éthiques relevant 1) de la société du numérique; 2) de la gouvernance des données et 3) du développement et de l'implantation des systèmes d'intelligence artificielle, en insistant spécifiquement sur les enjeux des technologies mobilisant l'informatique affective. Parfois traités conjointement en raison des nombreux chevauchements entre les domaines de la gestion des données et de l'intelligence artificielle, et à d'autres moments séparément en raison de leurs particularités inhérentes, les enjeux qui suivent adressent les différentes pratiques de gestion des données personnelles, leurs implications à l'échelle individuelle et sociétale, ainsi que les risques associés à l'utilisation de technologies d'informatique affective qui, nous le verrons, exploitent certaines de nos vulnérabilités humaines (Sullins, 2012).

2.1 Enjeux éthiques et sociaux de la société du numérique

La présente section dressera le portrait de l'industrie du Big Data. À travers les différentes sous-sections, nous adresserons les enjeux relatifs aux différentes utilisations que l'industrie fait des données personnelles ainsi que leurs conséquences sur les individus qui, nous le verrons, n'ont que très peu de pouvoir dans l'écosystème.

2.1.1 Le marché vorace des données et le *Far West* de la transition numérique

L'article de Someh et al. (2019) dépeint une industrie coercitive. Les auteurs dénoncent le fait que la participation des individus à la société soit contingente à leur apport en données personnelles à l'industrie. Effectivement, comme elles sont imbriquées dans le quotidien des individus, les

technologies deviennent « difficiles à éviter » (Someh et al. 2019, traduction libre : 730). Alors que les utilisateurs ont appris à dépendre de celles-ci, ils se voient forcés à partager leurs données, non seulement pour y avoir accès (Newell et Marabelli, 2015; Someh et al., 2019; Crawford et al., 2014), mais aussi pour répondre aux attentes de la société (Richterich, 2018). Certains auteurs s'inquiètent également que la pression de divulguer ses informations personnelles ne se transforme en norme implicite et que cet automatisme ait des effets néfastes sur la minorité qui ne s'y conforme pas ainsi que les utilisateurs plus soucieux de leur vie privée (Martin, 2015; Newell et Marabelli, 2015). La question qui se pose est donc la suivante : si le refus d'obtempérer coûte aux individus leur participation active à la société et les condamne à l'isolement, ont-ils réellement le choix (Zuboff, 2015; Someh et al. 2019)? Pour Someh et al. (2019), cette participation n'a effectivement rien de volontaire.

De leur côté, Breidbach et Maglio (2020, traduction libre) parlent d'une « culture de prédation des données » qui illustre, entre autres, l'attitude agressive avec laquelle les corporations abordent la collecte de données (Martin, 2015). La quantité toujours grandissante de données disponibles ainsi que l'amélioration des capacités d'analyses des données massives motivent les organisations à collecter toujours plus d'informations (Richards et King, 2014). Bon nombre d'entre elles, pour qui « rien n'est trop trivial ou éphémère », conçoivent leurs produits et services de sorte à pouvoir en extraire le maximum de données personnelles sans même n'avoir d'utilité prévue pour celles-ci (Zuboff, 2015, traduction libre : 79; Someh et al., 2019; Breidbach et Maglio, 2020). La devise est simple: « *if it might be useful, record and store it* » (Hand, 2018, p. 180). Si la quantité de données peut effectivement aider les algorithmes à produire de meilleures prédictions (Mai, 2016), cette approche va à l'encontre du principe de minimisation des données défini par le règlement général sur la protection des données (Breidbach et Maglio, 2020). Officiellement adopté par l'Union Européenne le 25 mai 2018 et considéré comme étant la régulation la plus rigoureuse au monde en matière de protection des données (McStay, 2020), le texte de loi mentionne que « les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes » ainsi qu'« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Martin souligne qu'une partie des conséquences néfastes vient du fait que ces pratiques sont répandues à travers l'industrie et que « tout le monde le fait » (Martin, 2015, traduction libre : 75). Elle renchérit en disant que « les torts causés [par ces pratiques adoptées en bloc] sont plus grands que la somme [de ceux] causés par les firmes individuelles » (Martin, 2015, traduction libre : 77; Someh et al., 2019). Elle souligne que celles-ci sont nourries par « les demandes destructrices » d'approvisionnement massif en données personnelles que les *data customers* exercent sur les organisations de premier rang (Martin, 2015). Largement inconnues du grand public, ces organisations œuvrent dans l'ombre des produits et services légitimes des organisations du marché primaire et poussent ces dernières à adopter des stratégies non éthiques de sorte à extraire un maximum de données personnelles des consommateurs (Martin, 2015). Adoptées et largement acceptées par tous, ces pratiques devenues légitimes entraînent « un effet négatif en chaîne » sur l'ensemble de l'industrie (Someh et al., 2019, traduction libre : 727).

À lumière des faits présentés ci-haut, il est évident que les données personnelles sont dorénavant perçues comme des actifs commerciaux sur lesquels toutes les corporations veulent mettre la main (Someh et al., 2019). Comme nous le verrons en deuxième partie de cette revue, elles sont vendues et partagées *ad vitam æternam* sans jamais ne perdre de valeur et représentent une source d'enrichissement intarissable pour les grands joueurs d'une économie de plus en plus digitale (Someh et al., 2019; Spiekermann, Acquisiti, Bohme et Hui, 2015). Comme le soulignent Someh et al. (2019, traduction libre : 727), les « énormes avantages financiers et commerciaux » que représentent les données pour les organisations sont une source de motivation pernicieuse qui pousse à l'utilisation des données à des fins néfastes, comme celles qui seront abordées dans les sections suivantes.

2.1.2 Individualité et société

Illusion de liberté

L'accès à d'énormes quantités d'informations personnelles d'une granularité spectaculaire ainsi que la capacité d'orienter le contenu utilisateur permettent aux organisations de manipuler ces derniers jusqu'à ce qu'ils manifestent les comportements désirés, souvent à des fins économiques qui ne bénéficient qu'à elles seules (Someh et al., 2019). Martin (2015 : 73) rapporte l'expression

« *digital market manipulation* » utilisée par Ryan Calo (2014) pour décrire la connaissance incroyablement pointue que les organisations ont de leurs utilisateurs. Sans aucun scrupule, ces dernières exploitent les vulnérabilités personnelles que révèlent les données de leurs utilisateurs pour influencer leur expérience de façon hautement ciblée (Martin, 2015).

Le terme « *filter bubble* » originalement employé par Pariser (2011, cité de Richterich, 2018) est utilisé pour dépeindre les conséquences de l'hyperpersonnalisation du contenu utilisateur sur l'exposition de ces derniers à la diversité et leur liberté de choix (Richterich, 2018; Breidbach et Maglio, 2020; Breidbach et al. 2019). Les craintes sont qu'à long terme les utilisateurs baignent dans un environnement qui renforce leurs points de vue et qui ne les oppose que très peu (Richterich, 2018). À cet effet, Newell et Marabelli (2015) questionnent ce que l'exposition à un contenu qui renforce nos croyances et qui s'accorde parfaitement à nos préférences fera à notre tolérance envers la différence. Ils soulèvent les abus et l'exploitation auxquels ces pratiques peuvent mener, ainsi que les dangers qu'elles peuvent représenter pour les populations plus vulnérables. Les auteurs soulignent que l'interférence des organisations sur le contenu offert aux utilisateurs puisse mener au changement progressif des opinions du public, « de la vision du monde des consommateurs, ainsi qu'à de nouvelles formes de discrimination » (Newell et Marabelli, 2015, traduction libre : 8).

Ces propos révèlent le rôle important que les plateformes de médias sociaux et les corporations jouent sur « la formation d'opinions, la prise de décision et leur participation discursive », mais également leur influence dans la production de données (Richterich, 2018, traduction libre : 48). Effectivement, Richterich (2018) nous fait remarquer qu'à force que l'utilisateur rencontre et interagisse avec le même contenu, les données dérivées de ces interactions sont susceptibles de renforcer son profil. Il continue alors de recevoir le même type de contenu, un peu à la façon d'une « chambre d'écho », réduisant toujours plus la diversité d'information qu'il reçoit (Pariser, 2011, cité de Richterich, 2018, traduction libre : 47). De cette façon, l'industrie du Big Data participe fortement à la construction de l'image du bon citoyen, qu'elle forge à son avantage et ses bénéfices, et « pousse le jeu de l'ingénierie sociale à un tout autre niveau » (Ekbia et al. 2015, traduction libre : 1538).

Épiés et contrôlés

Comme l'argumentent plusieurs auteurs, les faits pointent vers l'émergence d'une « société de surveillance » (Breidbach et al., 2019, traduction libre : 670; Someh et al., 2019) qui « observe, suit, mesure et profile la vie des individus » (Someh et al., 2019, traduction libre : 730), mais aussi qui régule et contrôle le comportement de ces derniers (Breidbach et al., 2019; Someh et al., 2019). Cette société est lourdement dénoncée par l'auteure Shoshana Zuboff (2015, traduction libre : 75) qu'elle qualifie de « surveillance capitaliste ». Cette « société de surveillance » est notamment possible grâce à l'étendue des informations disponibles et recueillies par des organisations dont les utilisateurs n'ont aucune conscience (Martin, 2015). Ce contexte génère l'impression répandue que le Big Data est « omniprésent, omniscient » et qu'on ne peut y échapper, elle devient donc un moyen de contrôle et de régulation hautement efficace (Martin, 2015, traduction libre : 78; Someh et al., 2019).

Martin (2015, traduction libre : 77) nous dit que « le simple fait de croire [être] observé suffit pour que les individus agissent comme s'ils étaient surveillés », signifiant donc que l'industrie du Big Data peut compter sur l'ensemble des individus, incluant ceux qu'elle ne surveille pas activement, pour se comporter d'une façon qui l'avantage. Cette « société de surveillance » qui laisse planer la possibilité d'une intrusion de la vie privée (Hand, 2018) entrave le besoin des individus « de ne pas être observés, ainsi que [leur besoin] d'être uniques et de se sentir eux-mêmes » (Martin, 2015, traduction libre : 77; Someh et al. 2019). Elle empiéterait également sur leur espace personnel, espace qui leur assure « un mouvement physique et intellectuel sans contraintes et sans regard [lui permettant de] se développer [et de] cultiver des relations », brimant alors l'expression de leur individualité (Martin, 2015, traduction libre : 77). Effectivement, l'impression d'être constamment observé peut nuire au « sentiment de liberté et d'autonomie » des individus, ainsi qu'à leur « sentiment de contrôle » sur leur vie (Newell et Marabelli, 2015, traduction libre : 7). Martin (2015, traduction libre : 77) ajoute que « la peur d'être observé et jugés par les autres [influence la façon dont] les individus se comportent et pensent » dans les sphères susceptibles d'être surveillées. De leur côté, Newell et Marabelli (2015) soulignent le risque que cette conscience élevée du regard potentiel de l'autre puisse nous amener à modifier nos comportements et prendre moins de risque ou encore éviter de s'exposer à l'échec.

De son côté, González Fulter (2010) s'attarde à l'utilisation de techniques de *data mining* à des fins de surveillance. L'auteure souligne que « le traitement des données personnelles de milliers de personnes » sert à créer des catégories et à déterminer « [lesquelles] seront considérées comme déviantes, potentiellement suspectes, placées sous plus haute surveillance, ou encore arrêtées et fouillées » (González Fulter, 2010, traduction libre : 92). Martin (2015, traduction libre : 73) dénonce la tendance à classer les individus sous des catégories aux appellations irrespectueuses à devenir « un exercice d'objectification » de l'individu qui réduit son identité à une « simple catégorie » parfois lourde de signification et stigmatisante. González Fulter (2010, traduction libre : 92) souligne qu'à travers ce traitement massif des données personnelles, les données des uns servent d'arme de discrimination et d'incrimination pour les autorités et les organisations qui les utilisent afin de « construire la définition des minorités suspectes ».

L'auteure dénonce le discours habituel qui incombe à l'individu de fournir des données exactes dans le but d'améliorer l'efficacité et la performance des mesures de sécurité publique (González Fulter, 2010). Dans les faits, ces mesures dissimulent souvent l'utilisation des données recyclées des grandes corporations et à des fins autres que pour celles consenties, comme la surveillance (González Fulter, 2010; Boyd et Crawford, 2012). Dans ce contexte, l'excuse de la responsabilité citoyenne maintiendrait l'individu dans l'ombre et le contraindrait à participer à cette « société de surveillance » malgré lui (González Fulter, 2010; Hand, 2018; Breidbach et al., 2019, traduction libre; Someh et al., 2019).

Données personnelles

L'industrie des technologies se développe à une vitesse fulgurante. Avec les nouvelles capacités technologiques et les utilités auxquelles elles sont mises, les notions de vie privée et de confidentialité sont appelées à être redéfinies constamment (Ekbia et al., 2015). L'ère du Big Data entraîne une série d'enjeux inattendus, dont plusieurs concernent la vie privée et sortent largement du cadre de référence actuel en matière de réflexion, de protection et de régulation qui entoure le sujet (Ekbia et al 2015).

À titre d'exemple, Mai (2016) rapporte la notion de « confidentialité d'informations » correspondant à la définition originale de Westin (1967, cité de Mai, 2016, traduction libre :

194) qui veut que « la confidentialité [soit] la revendication des individus, des groupes ou des institutions à déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées à d'autres ». Comme nous le verrons tout au long de cette revue de littérature, la complexité de l'industrie du Big Data, l'évaporation du consentement et le manque de contrôle sur les données rendent pratiquement impossible d'honorer cette définition et les principes qui la sous-tendent. Aussi, au cœur de la définition de celle-ci réside la notion de donnée personnelle qui, à l'ère du Big Data, est loin d'être étanche.

Le *RGPD* (2016, ch. 1, art. 4) définit les données à caractère personnel de la façon suivante :

> « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Hand (2018, traduction libre : 181) soulève certaines complexités relatives au fait que « les données n'existent pas de façon isolée, mais dans un contexte », compromettant l'exhaustivité de la définition donnée par le RGPD. Effectivement, l'auteur souligne les nombreux chevauchements entre les données personnelles des individus, dans le sens où les données personnelles de l'un peuvent décrire d'autres individus et révéler des informations personnelles à propos de ces derniers, ce que Barocas et Nissenbaum (2014, traduction libre : 61) appellent « la tyrannie de la minorité ». L'enjeu a souvent été rapporté dans le domaine de la recherche médicale par exemple, lorsque le traitement des données génomiques d'individus peut révéler des informations personnelles sur des membres de sa famille et compromettre leur vie privée (Ekbia et al. 2015; Hand, 2018). L'auteur souligne notamment que :

> « [les] données personnelles [de l'un] peuvent inclure le fait que [l'un] appartient à un groupe en particulier. Par contre, le fait que ce groupe se soit rencontré à un moment et un endroit précis n'est pas une donnée personnelle en soi. Cependant [le fait de] mettre ces données ensemble [peut permettre de] déduire où [l'individu] était. Combiner [les] données

> personnelles [de l'un] à d'autres données [donne] plus de données personnelles à propos de [cette personne] » (Hand, 2018, traduction libre : 181).

En plus d'illustrer les chevauchements entre les données personnelles de l'un et celles de l'autre, le passage précédent révèle une portée beaucoup plus large à la notion de données personnelles que précédemment conçue. Effectivement, le traitement de ces données a des implications importantes pour la notion de vie privée de groupe longtemps oubliée dans la question de l'équilibre entre la vie privée des individus et la sécurité publique (Floridi, 2014; Zwitter, 2014; Richterich, 2018). Les besoins de considération pour ce niveau de vie privée sont pressants puisque, mêmes lorsque les données sont anonymisées et que leur partage ne représente supposément plus de danger pour la vie privée de l'individu, celles-ci « [révèlent] beaucoup [d'informations] à propos de groupes spécifiques » qui possèdent également une grande valeur pour les entreprises (Zwitter, 2014, traduction libre : 4).

La définition de la notion de données personnelles comme entendu par le RGPD pose également problème dans le cas des données issues des technologies d'informatique affective. Les données qu'elles traitent sont considérées comme « fondamentalement personnelles et privées, peut-être même plus que les pensées » (Picard, 2003, traduction libre : 61). Effectivement, les données issues d'émotions offrent un regard privilégié sur la vie interne des utilisateurs qui leur est parfois inconnu à eux-mêmes (Brigham, 2017, Feldman Barrett et al., 2019). Certaines technologies particulièrement intrusives comme l'interface neuronale affective directe peuvent même révéler des informations que les individus n'ont pas envie de partager compromettant alors l'intimité mentale de ceux-ci (Steinert et Friedrich, 2020). La nature sensible de ces informations peut générer un inconfort à l'idée qu'elles puissent être accédées et manipuler par d'autres personnes que soi, pouvant être perçu comme une « intrusion de l'espace personnelle émotionnelle » (Duffy, 2008, traduction libre : 27).

Si l'intuition première est que ces données intimes sont des données personnelles, le RGPD ne fait aucune mention des émotions (McStay, 2020). Sont-elles réellement considérées comme telles? Le texte de loi définit les données biométriques comme étant :

> « [des] données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques; » (RGPD, chap. 1, art. 4, par. 14).

Le RGPD exclut donc de sa protection toutes technologies ne traitant pas des données personnelles et à des fins pouvant mener à l'identification (McStay, 2020). Tombant plutôt dans la catégorie de la biométrie « douce » définie par « l'utilisation de traits communs ne permettant pas de distinguer ou d'identifier clairement un individu » (Article 29 Data Protection Working Party, cité dans McStay, 2020, traduction libre : 4), les données issues d'émotions et les technologies qui les traitent ne seraient donc pas couvertes par le RGPD (McStay et Urquhart, 2019; McStay, 2020).

L'attention particulière que porte le RGPD à l'identification des individus, qu'il semble considérer comme la source principale de risques pour la vie privée, se fait au détriment des torts potentiels que portent tous les autres types de données (Barocas et Nissenbaum, 2014; McStay et Urquhart, 2019; McStay, 2020). Cette exclusion est contre-intuitive puisqu'elle offre la place à des pratiques qui compromettent la vie privée, alors qu'il est supposé les prévenir (McStay, 2020).

L'illusion de vie privée

La question de la vie privée est souvent abordée sous deux angles : celui de l'accès limité et celui du contrôle (Mai, 2016; Richterich, 2018). La prémisse de la première approche soutient que l'individu est en mesure d'ériger des zones à l'intérieur desquelles il peut jouir d'une vie privée et par le fait même limiter l'accès aux informations qui le concernent. La deuxième approche suppose la capacité de l'individu de contrôler l'accès des autres à ses informations personnelles (Mai, 2016; Richterich, 2018). Mai (2016, traduction libre : 195) souligne que la conceptualisation de la vie privée comme une capacité individuelle « de limiter l'accès à ou de contrôler ses informations personnelles » attribue faussement la responsabilité et le choix de défendre ce droit aux individus et épargne les organisations de leur responsabilité morale à leur égard (Richterich, 2018). La notion de responsabilité semble également aller à l'encontre du droit civique que représente la vie privée dans toute société démocratique, droit duquel « la protection des données tend à être considérée comme une extension » et pour lequel l'individu ne devrait pas avoir à déployer d'effort

(Richterich, 2018, traduction libre : 35; Mai, 2016). La question de la responsabilité individuelle à l'égard de la vie privée est complexifiée par celle de la propriété des données personnelles, sujet que nous traiterons davantage en deuxième partie de cette revue . Effectivement, la possibilité et le désir que l'individu puisse pleinement posséder ses données personnelles de façon exclusive viennent inévitablement déposer la responsabilité de la protection de la vie privée entre les mains de ce dernier et la retirer de celles des corporations (Ekbia et al. 2015). Cependant, en plus de bombarder l'utilisateur d'une quantité phénoménale d'informations au quotidien, l'industrie du Big Data présente des déséquilibres de pouvoir et une asymétrie des connaissances (Someh et al., 2019) qui le limite lourdement dans sa « capacité de prendre […] des décisions conscientes » à l'égard de ses informations personnelles (Mai, 2016, traduction libre : 196). Alors que l'industrie du Big Data exerce une influence invisible constante et puissante, comment pouvons-nous espérer assurer la lourde responsabilité de la protection de la vie privée à l'échelle individuelle?

Le droit à la vie privée semble effectivement contingent à plusieurs facteurs ainsi que dépendre de forces dépassant largement l'individu (Mai, 2016). Richterich (2018) note en exemple les restrictions prévues par le *RGPD* (2016, sec. 3, art. 17, par. 3) qui s'appliquent au droit à l'oubli. Le paragraphe stipule notamment que :

> « Les paragraphes 1 et 2 [(qui désignent le droit à l'effacement, les motifs pour lesquels il peut être invoqué ainsi que les obligations du responsable du traitement)] ne s'appliquent pas dans la mesure où [le] traitement est nécessaire à : a) l'exercice du droit à la liberté d'expression et d'information […], c) pour des motifs d'intérêt public dans le domaine de la santé publique […] ».

Le *RGPD* (2016, cons. 73) s'étend au sujet des limitations applicables à certains droits, dont celui à l'effacement, et mentionne entre autres que :

> « Des limitations à certains principes spécifiques ainsi qu'au droit à l'information, au droit d'accès aux données à caractère personnel, au droit de rectification ou d'effacement de ces données […] peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité

> publique [...] y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces […], et pour garantir d'autres objectifs d'intérêt public importants ».

Si parfois la vie privée « se heurte à l'importance de l'utilisation des données pour promouvoir le bien commun » (Hand, 2018, traduction libre : 186), la critique concerne le fait que l'applicabilité des limitations prévues par la loi soit laissée entre les mains des grandes corporations qui décident à quel moment le droit de l'individu à l'égard de sa vie privée entrave leur liberté d'expression ou la sécurité publique (Richterich, 2018). La question de l'équilibre entre la vie privée des individus et la sécurité publique est longuement abordée dans la littérature. González Fulter (2010) déplore l'utilisation des techniques d'exploration des données sous le prétexte du combat contre le terrorisme, alors que les bénéfices de ces systèmes pour la sécurité publique sont beaucoup moins tangibles que leurs retombées néfastes pour la vie privée des individus. Hand (2018, traduction libre : 180) pour sa part souligne que si les systèmes de surveillance se prouvent effectivement précieux dans la chasse aux terroristes, ils le sont également « pour traquer les [individus] respectueux de la loi qui ont des opinions qu'un gouvernement pourrait moins apprécier », notant les lourdes conséquences que le fait de donner préséance à la défense du bien commun peut avoir sur la vie privée des individus (Richterich, 2018). De façon intéressante, London (2003, cité dans Richterich, 2018, traduction libre : 36) nous dit que la réponse appropriée à la défense du bien commun dépend « de la compréhension des valeurs [qui sont] liées au bien commun ». À cet égard, les organisations ont tout intérêt à démontrer l'apport de l'industrie du Big Data au bien-être de la société. Effectivement, cet apport devient un motif légitime pour la collecte extensive que les organisations font des données personnelles qui, pour leur part, sont habilement décrites comme des contributions impératives au bien commun (Richterich, 2018).

La protection de la vie privée n'est donc pas un droit aussi acquis qu'il en a l'air. Mai (2016, traduction libre : 196) souligne que la définition de la valeur de la vie privée demeure floue et « ouverte à de multiples interprétations ». Dans les faits, la vie privée se révèle hautement conditionnelle et très relative (Hand, 2018). Selon Hand (2018, traduction libre : 186), elle serait « dépendante du contexte et de la relation [entre deux personnes], ainsi que de l'usage à laquelle les données sont soumises ». Kokolakis (2017) abonde en ce sens et souligne que les individus

sont susceptibles de se comporter différemment à l'égard de la vie privée dans différents contextes. L'auteur nous dit également que la notion d'information personnelle « n'est pas un objet cohérent, [qu'il y en a] plusieurs types et que les individus attribuent différentes valeurs à ceux-ci ». Il souligne également le rôle que la sensibilité des informations personnelles peut jouer dans l'équation (Kokolakis, 2017, traduction libre : 126). Par exemple, issues d'émotions, les données qu'exploitent les technologies d'informatique affective offrent un regard privilégié sur la vie interne des utilisateurs qui leur est parfois inconnu à eux-mêmes (Brigham, 2017, Feldman Barrett, Adolphs, Marsella, Martinez et Pollak, 2019). Ces technologies, dont certaines sont particulièrement intrusives comme les INAD, peuvent révéler des informations que les individus n'ont pas envie de partager et compromettre leur intimité mentale (Steinert et Friedrich, 2020).

La valeur relative de la vie privée est à la base d'un phénomène appelé le « paradoxe de la vie privée » qui s'articule autour du fait que « les technologies permettent souvent de protéger la vie privée d'une main tout en créant des risques d'atteinte à la vie privée avec l'autre » (Wittes et Liu, 2015, traduction libre : 3). Selon Wittes et Liu (2015), les utilisateurs décident de prendre part à certaines de ces technologies sur la base de « la valeur qu'ils accordent à la vie privée donnée ou à [celle] retirée » par ces technologies (Wittes et Liu, 2015, traduction libre : 3). Cette valeur serait accordée en fonction de l'audience de qui nous souhaitons garder certaines informations privées et peut mener à une vie privée dont la valeur, dans les faits, diffère grandement de celle qui est débattue par les militants de la cause sur la scène publique (Wittes et Liu, 2015). Les préférences des individus quant à leur vie privée sont hautement hétérogènes (Spiekermann et al., 2015) et ceux-ci ne se cachent pas des mêmes choses ni des mêmes personnes (Wittes et Liu, 2015). Effectivement, une « technologie utilisée de la même façon par deux personnes différentes peut éroder la vie privée [de l'une] et améliorer [celle de l'autre] » (Wittes et Liu, 2015, traduction libre : 9). Les auteurs offrent l'exemple d'un individu qui cherche à faire sens de sa sexualité à travers son moteur de recherche Google. Les auteurs remarquent qu'il est possible que ce dernier valorise davantage sa vie privée à l'égard de sa famille et accorde moins d'importance à l'inconnu chargé d'analyser ses données (Wittes et Liu, 2015). La capacité de pouvoir faire ce choix entre ces deux types de vies privées est un bénéfice considérable pour l'individu qui, faute d'accès à une plateforme qui lui permette de naviguer ce sujet sensible en toute confidentialité et par peur de s'exposer, n'aurait peut-être jamais eu réponse à ses questions (Wittes et Liu, 2015). La perception

du comportement de l'individu à l'égard de sa vie privée comme « un échange bien équilibré et conscient en faveur de la facilité » ou encore du bénéfice appelle à la vigilance selon Andrejevic (2014, traduction libre : 1682). Effectivement, cette interprétation ferait fi des nombreuses forces à l'œuvre qui dépassent largement l'individu (Mai, 2016) et l'empêchent d'être pleinement conscient des implications de cet échange (Andrejevic, 2014).

González Fulter (2010) considère la possibilité qu'acculé au pied du mur et présenté avec un faux choix en ce qui a trait à la protection de sa vie privée, l'individu puisse choisir une autre alternative. Effectivement, confronté au choix entre l'accès à des services qui récoltent souvent plus d'informations personnelles que nécessaire et la protection de ses informations personnelles au coût cher payé de sa participation à la société (Zuboff, 2015; Someh et al., 2019), ce dernier pourrait choisir de « fournir des informations personnelles inexactes » (González Fulter, 2010, traduction libre : 90). Outre l'incitation à mentir que ce faux choix peut produire, l'auteure souligne le potentiel de cette stratégie dans un contexte où « la construction de connaissance [à propos des individus et de la société en général] […] s'appuie de plus en plus sur la génération externe de conclusions basées sur des inférences qui ne sont pas toujours claires » (González Fulter, 2010, traduction libre : 91). Effectivement, permettre aux individus d'interférer avec le degré d'exactitude des données personnelles recueillies en manipulant les traces digitales qu'ils laissent sur leur passage « contribuerait à la justesse des connaissances déduites par le système » et permettrait à ces derniers de « jouer [un rôle] dans leur représentation et définition de soi, ainsi que dans la définition des catégories affectant les autres » (González Fulter, 2010, traduction libre : 91; Ekbia et al. 2015).

2.1.3 Structures de pouvoir et domination des données

L'industrie du Big Data accentue les écarts existants dans notre société et offre encore plus de terres à conquérir à une petite minorité (Richterich, 2018). Effectivement, le marché des données est dominé par une poignée de grandes corporations dont les moyens financiers donnent accès à des ressources que peu peuvent se procurer, tout en jouissant des solutions performantes bon marché desquelles la majorité des joueurs de l'industrie doivent dépendre (Ekbia et al. 2015). Ce sont également elles qui ont la mainmise sur les banques de données tant convoitées et qui, sous le prétexte de la protection de la vie privée (Richterich, 2018), exercent un pouvoir restrictif sur

leur accès (Boyd et Crawford, 2012). Dans les faits, cet accès exclusif est réservé à ceux qui en ont les moyens et dont les intérêts et les intentions s'alignent avec celles des corporations, creusant davantage le fossé apparent entre les « *big data rich* » et les « *big data poor* » (Boyd et Crawford, 2012, traduction libre : 674). L'accès aux banques de données est toujours permis aux mêmes universités prestigieuses et centres de recherche qui produisent de nouvelles connaissances destinées à être réinjectées dans l'industrie, et ce sous le contrôle et au profit des grandes corporations (Boyd et Crawford, 2012; Richterich, 2018).

Cette minorité qui produit les résultats de recherche est particulièrement homogène (Boyd et Crawford, 2012; Richterich, 2018). En effet, elle privilégie ceux « qui peuvent lire les chiffres » ce qui, encore aujourd'hui, désigne une majorité d'hommes (Boyd et Crawford, 2012, traduction libre : 674). Par le fait même, ce que la minorité exclut de son cercle sont les perspectives divergentes et les connaissances issues de domaines comme les sciences sociales, ainsi que la richesse et l'apport qu'un point de vue féminin correctement représenté peuvent amener. Ces recherches demeurent donc incontestables et incontestées par une grande diversité d'acteurs dont les moyens limitent la capacité d'en vérifier la méthodologie, d'en reproduire les résultats et, ultimement, d'en assurer la fiabilité (Boyd et Crawford, 2012; Richterich, 2018). Cette situation crée ce que Boyd et Crawford (2012, traduction libre : 674) appellent une « culture restreinte de résultats de recherche » ayant toutes les raisons de susciter la méfiance d'un public contraint à rester dans l'ombre quant aux « possibilités et aux risques du Big Data » (Richterich, 2018, traduction libre : 40; Hand, 2018). Thatcher (2014 : 1766) dépeint la situation de façon éloquente en nous disant que « *the very limits of knowledge are set through the data infrastructure of private corporations* ».

Maintenus dans l'ombre

Comme Richterich (2018, traduction libre : 40) le souligne, « le Big Data est une ressource essentielle pour faire sens du monde à l'ère numérique ». Maintenant, la littérature nous indique que cette ressource est loin de bénéficier tout le monde. Effectivement, les capacités l'industrie du Big Data ont connu des « développements rapides [qui] dépassent la compréhension humaine » (Zuboff, 2015, traduction libre : 83). Cette conscience « à la traîne » reflète des déséquilibres importants qui nécessitent d'être abordés (Breidbach et al., 2019, traduction libre : 671).

Comme Someh et al. (2019, traduction libre : 726) l'indiquent, la conscientisation fait référence à « ce que les individus savent et comprennent [du Big Data et] de l'analytique des données massives, [par exemple] la façon dont les organisations analysent leurs données pour offrir des produits et des services », ce qui, dans les faits, s'avère à n'être que très peu. Par défaut, l'industrie du Big Data et les technologies qu'elle utilise sont d'une complexité qui défie « les capacités intellectuelles » de la majorité (Mai, 2016, traduction libre : 197), ce qui constitue un premier frein notable à l'enjeu en question. Cependant, la possibilité d'une conscientisation du public est aussi lourdement entravée par le pouvoir démesuré que détiennent les corporations de l'industrie (Richterich, 2018; Breidbach et al., 2019; Someh et al., 2019). Ce pouvoir, acquis grâce à l'asymétrie de connaissances, l'opacité des pratiques et la détention d'un savoir exclusif, permet à ces dernières d'exploiter et de maintenir l'ignorance et l'impuissance du public (Richterich, 2018; Someh et al.,2019; Breidbach et Maglio, 2020).

La relation profondément déséquilibrée que l'industrie maintien avec ses utilisateurs n'en est qu'un exemple. Effectivement, ces derniers sont scrutés par les corporations au point où « [elles] apprennent à [les] connaître mieux qu'ils ne se connaissent eux-mêmes » (Someh et al., 2019, traduction libre : 729; Zuboff, 2015). Alors qu'un niveau de transparence toujours plus grand est exigé de la part des utilisateurs qui se font soutirer toujours plus d'informations, les corporations sont loin de rendre la pareille (Richterich, 2018). Effectivement, le manque de transparence avec lequel l'industrie opère n'offre que très peu d'opportunités pour l'utilisateur de « s'informer sur l'analytique des données massives, son fonctionnement et la façon dont elle influence [ses] choix et [ses] comportements » (Someh et al., 2019, traduction libre : 726; Crawford et al., 2014; Breidbach et Maglio, 2020).

Les utilisateurs sont donc délibérément maintenus à l'écart par une industrie qui restreint l'accès aux connaissances, autant physiquement qu'intellectuellement (Richterich, 2018; Mai, 2016; Hand, 2018). Comme le soulignent Someh et al., (2019, traduction libre : 726), « les [utilisateurs] doivent savoir quelles données les organisations collectent à leur sujet, qui possède et contrôle ces données, et quels tiers y ont accès » (Someh et al., 2019, traduction libre : 726). Ces informations sont volontairement dissimulées par les organisations sous le couvert d'un vocabulaire inaccessible et qui ne résonne qu'avec une très petite minorité (Andrejevic, 2014; Hand, 2018). L'information disponible se résume souvent à celle contenue dans des politiques de vie privée alourdies de termes

légaux qui dépassent largement la compréhension du public (Hand, 2018; Someh et al., 2019). Comme le pointent judicieusement Barocas et Nissembaum (2014, traduction libre : 60) « qu'est-ce que peut signifier, pour une personne ordinaire, le fait que [ses] informations seront partagées avec […] la NSA [par exemple]? ». Alors que ces informations sont habituellement divulguées dans les politiques de vie privée, elles sont loin d'être suffisantes et ne couvrent pas les implications de ces pratiques, informations qui, elles, sont impératives pour aider l'utilisateur à comprendre les conséquences de l'utilisation de ses données (Andrejevic, 2014; Barocas et Nissenbaum, 2014; Someh et al., 2019).

Alors que la conscience s'éveille lentement, la majorité des individus n'ont aucune idée des conséquences potentielles des pratiques d'une industrie qui les maintient volontairement dans l'ombre (Someh et al., 2019; Breidbach et al., 2019). Dérobés de leur liberté de choix et de leur sentiment d'agence en ce qui a trait à leurs données (Breidbach et Maglio, 2020), les utilisateurs se retrouvent en position de vulnérabilité, prêts à non seulement servir de ressources, mais également de cibles pour une industrie dont la soif est inétanchable (Zuboff, 2015).

2.2 Enjeux éthiques liés à la gouvernance des données

La section qui suit nous permettra de soulever des enjeux éthiques présents à différentes étapes du cycle de vie des données. Plus précisément, nous débuterons en adressant la question du consentement, du partage, de la propriété ainsi que de la sécurité des données personnelles. Nous enchaînerons ensuite avec les enjeux méthodologiques qui, nous le verrons, comportent leur lot d'implications éthiques. Nous aborderons les sujets de la qualité des données, des biais méthodologiques et algorithmiques, de la fiabilité des inférences algorithmiques, ainsi que les potentielles discriminations qui peuvent en découler.

2.2.1 Le consentement pas toujours éclairé

Comme soulignée en première partie de revue de littérature, les acteurs de l'industrie abordent la collecte de données avec une attitude agressive dans la croyance que « plus d'informations est mieux » (Mai, 2016, traduction libre : 194). Cependant, la collecte implique aussi la notion de consentement, plus précisément de consentement éclairé, qui est fortement remise en question à la

vue des nombreuses avenues de recherches rendues possibles par le phénomène des données massives ainsi que « la croissance exponentielle […] de la puissance computationnelle » qui l'accompagne (Ioannidis, 2013, cité de Richterich, 2018, traduction libre : 45). Dans ce contexte aux mille opportunités, que l'on tente de rendre le consentement obsolète ou encore qu'on le néglige volontairement sous l'excuse de l'utilisation de données déjà existantes dans les banques de données collectées par les corporations n'est pas étonnant (Richterich, 2018). Hand (2018) remet en question l'applicabilité du consentement éclairé aujourd'hui. Effectivement, alors qu'il est habituellement obtenu avant une intervention et basé sur une bonne compréhension des implications et conséquences possibles, le consentement éclairé semble aujourd'hui aller à l'encontre de « l'essence même des promesses […] d'applications futures inconnues » du Big Data (Hand, 2018, traduction libre : 183).

Hand (2018, traduction libre : 183) souligne aussi deux conditions habituellement nécessaires pour considérer le consentement à l'égard de la collecte et l'utilisation des données utilisateurs « valable », soit « (1) une idée précise de l'usage qui pourrait être fait des données dans le futur et (2) une compréhension de la façon dont elles seront utilisées ». Selon lui, ces deux conditions posent problème. La première condition est entravée par l'impossibilité d'identifier les futures utilisations potentielles auxquelles les données pourraient être sujettes (Hand, 2018). Outre le fait que ces utilisations futures soient quasi infinies, il est impossible de quantifier l'apport ou le rôle que certaines données jouent dans la découverte de nouvelles informations suite à la fusion de banques de données (Hand, 2018). Alors que le consentement donné ne couvre pas toutes les finalités, la possibilité demeure que des analyses non consenties puissent révéler des informations importantes sur lesquelles l'humain a l'obligation morale d'agir, comme une situation d'abus (Hand, 2018). Cette éventualité soulève une foule de questions éthiques relatives à la confiance accordée à ce genre de prédiction, la responsabilité d'agir en cas de doute, la possibilité de porter jugement sur la base de prédictions peu fiables et d'envahir la vie privée des gens, ainsi qu'à toutes les conséquences qu'une mauvaise intervention ou le fait de ne pas intervenir peuvent engendrer (Zwitter, 2014). Aussi, comme les nouvelles données générées peuvent servir à prendre des décisions sur les individus, il est important que ces utilisations potentielles puissent être connues par ceux-ci avant qu'ils ne donnent leur consentement (Hand, 2018). Le *RGPD* (2016, cons. 33) tente d'adresser l'enjeu des applications futures inconnues des données (Hand, 2018) :

> « Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet. »

Bien que cette disposition du RGPD vise spécifiquement le domaine de la recherche, elle implique directement le domaine commercial et les entreprises de l'industrie. Effectivement, la majorité des chercheurs du domaine du Big Data obtiennent leurs données des grandes corporations qui collectent elles-mêmes les données utilisateurs à travers la prestation de leurs services (Boyd et Crawford, 2012; Richterich, 2018). Ces utilisations secondaires reliées à la recherche font partie des nombreux éléments que cachent les conditions d'utilisation et les politiques de vie privée des entreprises (Boyd et Crawford, 2012). Malgré que le *RGPD* (2016, ch. 2, art. 5, al. b) cite le domaine de la recherche scientifique dans les exceptions au principe de limitation des finalités, Boyd et Crawford (2012, traduction libre : 673) soulignent que « les chercheurs font rarement partie de l'audience imaginée par les utilisateurs ». Même si ces utilisations secondaires sont considérées comme légitimes par la loi de l'UE sur la protection des données personnelles, ces utilisations peuvent avoir des conséquences et méritent d'être connues par les individus visés (Boyd et Crawford, 2012).

La deuxième condition énoncée par Hand (2018) sur la compréhension de l'utilisation des données pose aussi problème dans la mesure où elle « assume que la personne [qui consent] possède l'expertise et les connaissances pour comprendre la façon dont [ses] données seront utilisées », ce qui est peu réaliste considérant la « complexité inhérente » des technologies utilisées (Hand, 2018, traduction libre : 184). Pourtant, le *RGPD* (2016, cons. 63) stipule que « toute personne concernée devrait avoir le droit de connaître et de se faire communiquer […] la logique qui sous-tend [l'] éventuel traitement automatisé [de ses données] et les conséquences que ce traitement pourrait avoir […] » (Hand, 2018). Dans les faits, ces dispositions sont gravement altérées par les entreprises qui, par manque de transparence, participent à accroître le manque de conscience et de connaissance des individus à l'égard de l'analytique des données (Breidbach et Maglio, 2020).

Steinert et Friedrich (2020) soulignent l'importance du consentement éclairé et la complexité que cette deuxième condition peut prendre dans un contexte de technologie hautement complexe comme l'INAD. Effectivement, cette technologie d'informatique affective profondément intrusive qui vise à détecter, influencer et stimuler les états affectifs des utilisateurs peut avoir des conséquences difficiles à saisir. Son utilisation peut devenir problématique lorsque les utilisateurs ne comprennent ce que cette technologie qui « permet la manipulation de [leurs] processus affectifs » et pouvant « entraver leur intégrité mentale » leur fait concrètement (Steinert et Friedrich, 2020, traduction libre : 359). Ces derniers soulignent que c'est exactement ce que le consentement éclairé est supposé prévenir (Steinert et Friedrich, 2020). Ils appellent eux aussi à la transparence du fonctionnement de ces technologies, que les deux auteurs considèrent comme nécessaire pour « prévenir les abus » et redonner une signification au consentement qui, comme souligné par Richterich (2018, traduction libre : 51), repose initialement sur « des valeurs morales comme l'autonomie et la dignité humaine » (Steinert et Friedrich, 2020, traduction libre : 363).

Martin (2015) souligne que les utilisateurs acceptent de divulguer leurs données avec un objectif en tête ainsi que des attentes à l'égard de la confidentialité de leurs données qui peuvent être bafouées lorsqu'elles sont partagées. Boyd et Crawford (2012, traduction libre : 672) abondent en ce sens, notamment lorsqu'elles disent : « Il est problématique pour les chercheurs de justifier leurs actions comme éthiques simplement parce que les données sont accessibles. Le fait que le contenu soit publiquement accessible ne signifie pas qu'il est destiné à être consommé par n'importe qui ». À cet effet, Richterich (2018, traduction libre : 44) ajoute que la question du consentement dans ce contexte « n'est toujours pas réglementée et [qu'] il n'est pas clair que l'approbation [à une politique de confidentialité sur une plateforme de] médias sociaux [soit équivalente à l'approbation de l'utilisation des mêmes] données à des fins de recherche ». Effectivement, l'auteure souligne que le consentement éclairé est souvent considéré comme un obstacle au progrès scientifique et une « entrave à l'innovation » (Richterich, 2018, traduction libre : 45). Dans ces conditions, le fait de ne pas consentir à l'utilisation de ses données serait même une « atteinte au bien public » selon certaines (Ioannides, 2013, cité de Richterich, 2018, traduction libre : 45; Crawford et al., 2014). Tout de même, ces justifications n'absolvent en rien la recherche de ses responsabilités morales à l'égard des données personnelles qu'elle traite et des individus que ces données décrivent selon Boyd et Crawford (2012).

2.2.2 Partage des données

Comme souligné plus haut, les données sont partagées entre les corporations et les institutions pour être réutilisées à des fins non consenties. L'industrie du Big Data est composée de plusieurs acteurs aux « propositions de valeurs complémentaires et adresse les besoins individuels de multiples bénéficiaires » (Breidbach et Maglio, 2020, traduction libre). Ces différents acteurs « s'approvisionnent en données » par l'entremise de plusieurs sources comme les utilisateurs de leurs produits et services et d'autres acteurs commerciaux desquels ils les achètent (Someh et al., 2019, traduction libre : 727). Cependant, souvent la pratique ne s'arrête pas là. Effectivement, en raison de la valeur qu'elles représentent, les données sont partagées et revendues sans retenue à d'autres acteurs au sein de l'écosystème à un point tel qu'il est pratiquement impossible de retracer leur provenance (Wixom et Ross, 2017; Hand, 2018). Les données proviennent donc de partout, littéralement (Someh et al., 2019).

Ce large « réseau de valeur » dans lequel le rôle et les intentions de chaque acteur diffèrent peut rendre « difficile l'identification du bénéficiaire clé des données », s'il y en a un (Breidbach et Maglio, 2020, traduction libre). Effectivement, les données personnelles sont d'intérêt pour une panoplie d'acteurs, notamment les *data customers* qui ont comme objectif premier de récolter les données personnelles des utilisateurs coûte que coûte (Breidbach et Maglio, 2020). Ces intentions parfois questionnables à l'égard des données motivent l'adoption de stratégies agressives et non-éthiques qui participent à créer et répandre la « culture de prédation des données » mentionnée en première partie de cette revue (Breidbach et Maglio, 2020, traduction libre).

Qui plus est, la pratique du partage des données est loin d'être transparente (Breidbach et Maglio, 2020; Breidbach et al., 2019; Someh et al., 2019). Effectivement, l'objectif réel derrière la collecte des données ainsi que les usages secondaires qui en sont faits sont souvent dissimulés derrière d'imposantes politiques de vie privée et des conditions d'utilisation « obscures » qui, alors qu'elles sont loin d'être exhaustives, atténuent considérablement la valeur du consentement des utilisateurs (Barocas et Nissenmbaum, 2014; Someh et al. 2019, traduction libre; Breidbach et al. 2019). Effectivement, ces documents sont si denses et complexes qu'ils ne sont que très rarement consultés par les utilisateurs qui, à la base, n'ont qu'une compréhension très sommaire des

implications relatives à l'analytique des données (Hand, 2018; Breidbach et Maglio, 2020). Leur « acquiescence par défaut » des conditions d'utilisation dont Hand (2018, traduction libre : 184) parle « assure la disponibilité et l'accessibilité de données [personnelles] qui peuvent être monétisées » de plusieurs façons par les corporations (Breidbach et Maglio, 2020, traduction libre; Wixom et Ross, 2017). En contrepartie, cela signifie que les utilisateurs restent dans l'ombre quant à ce qui arrive avec leurs données suite à leur collecte (Breidbach et al. 2019; Zuboff, 2015). Selon Breidbach et Maglio (2020), la situation dépeinte ci-haut a tout d'une relation d'exploitation. Effectivement, en plus de diminuer la conscience déjà quasi inexistante des utilisateurs à l'égard de l'analytique des données, le manque de transparence ainsi que la dissimulation volontaire des raisons qui motivent la collecte ont pour effet de contraindre les utilisateurs à accepter les termes proposés et les empêchent d'agir de façon complètement « libre et audotdéterminée » (Breidbach et Maglio; Someh et al., 2019, traduction libre : 726).

Considérant l'absence de contrôle de l'organisation initiale et des utilisateurs sur les données lorsqu'elles sont partagées, cette pratique qui semble n'avoir aucune fin peut engendrer des « préjudices de second ordre » qui découlent d'utilisations secondaires insoupçonnées « tels que le profilage, le suivi, la discrimination, l'exclusion, la surveillance gouvernementale » (Ekbia et al., 2015, traduction libre : 1536; Crawford, Milner et Gray, 2014; Someh et al., 2019; Breidbach et al. 2019). Les implications du manque de contrôle pour la vie privée des utilisateurs sont considérables alors que « la protection de l'identité [des] individus devient de plus en plus difficile […] à mesure que les organisations partagent [leurs données] » (Someh et al., 2019, traduction libre : 727; Zuboff, 2015). Ces implications sont d'autant plus importantes alors que les organisations de l'industrie utilisent l'analytique pour générer de nouvelles connaissances « qui peuvent révéler des informations sensibles et non désirées » au sujet des individus (Someh et al., 2019, traduction libre : 725). Ces nouvelles informations qui pourraient ne pas bien représenter ceux-ci peuvent également avoir des conséquences imprévues alors qu'elles sont partagées et réutilisées à des fins non-consenties (Someh et al., 2019; Mai, 2016). De façon intéressante, Mai (2016) souligne qu'à la suite de ces multiples partages et nombreuses manipulations, il n'est pas clair quels sont les droits de propriétés des différents acteurs à l'égard des données et nouvelles informations générées. Ce sujet est le point central de la section qui suit.

2.2.3 La propriété des données

Effectivement, qui possède ces données personnelles à propos des individus? Est-il même possible de leur attribuer une propriété individuelle? Partant de « l'interprétation des données personnelles comme un bien négociable », Spiekermann et al. (2015, traduction libre : 164) adressent l'enjeu et posent la question à savoir si « la vie des personnes, matérialisée dans leurs traces de données, peut être considérée comme une propriété ou si, en fait, les données personnelles doivent être considérées comme inaliénables des sujets de données » ? Cette question nous invite à réfléchir à l'enjeu que représente la tentative de réduire l'identité de l'homme à une chose, à ses comportements digitaux qui sont « datatifiables », analysables et monnayables (Cuckier et Mayer-Schoenberger, 2013, traduction libre : 29; Spiekermann et al., 2015).

Le RGPD traite de la question de propriété des données de façon implicite et semble se ranger du côté de la propriété personnelle des individus concernés. Effectivement, le considérant 7 (RGPD, 2016) du règlement stipule que « […] les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant », sans pour autant trancher sur la question laissant donc la porte ouverte à une panoplie d'acteurs pour revendiquer leur propriété (Hand, 2018; van Asbroeck et al., 2017, cité de Hand, 2018). Mai (2016) rapporte la position de Floridi (2006) qui veut que les données personnelles ne puissent être possédées. Effectivement, selon ce dernier, « les individus ne possèdent pas leurs données, ils sont leurs données » (Floridi, 2006; Mai, 2016, traduction libre : 195). L'auteur fait la différence entre le fait d'« appartenir à » et le fait de « posséder » et conclut que « les informations personnelles d'un individu lui appartiennent, au même titre que son corps et ses sentiments, mais qu'il ne les possède pas de la même façon qu'il possède sa voiture » (Floridi, 2006; Mai, 2016, traduction libre : 195). De son côté, Solove (2008, cité de Mai, 2016, traduction libre : 195) souligne que les « les informations personnelles sont souvent formées en relation avec les autres [et que] toutes les parties dans cette relation ont un droit quelconque sur ces informations ». Cette conception de la propriété des données soulève plusieurs complications qui font référence à la complexité « du cycle de valeur des données qui [implique] de nombreuses parties prenantes » (van Asbroeck et al., 2017, cité de Hand, 2018, traduction libre : 182). Effectivement, alors que ces complications ne sont à aucun moment adressées par la loi actuelle, toutes les manipulations auxquelles les divers acteurs soumettent les

données deviennent des motifs légitimes pour en revendiquer la propriété (van Asbroeck et al., 2017, cité de Hand, 2018).

2.2.4 La protection et la sécurité des données

Le phénomène du Big Data et de l'analytique des données massives entraînent des demandes notables et complexes en matière de performance auxquelles les techniques utilisées par les « approches plus traditionnelles d'intelligence d'affaires » ne peuvent tout simplement pas répondre (Basso, Mastsunaga, Moraes et Antunes, 2016, traduction libre : 165). Les nouveaux besoins de l'industrie « posent [donc] de nouveaux défis en matière de sécurité pour les normes, les méthodologies et les algorithmes traditionnels de cryptage des données » (Yang, Huang, Li, Liu, Hu, 2017, traduction libre : 21).

Les différentes pratiques de gestion des données personnelles, souvent effectuées « sans discernement et à des fins commerciales », ont parfois des conséquences néfastes qui reflètent d'importantes faiblesses au niveau de la sécurité et de la protection des données (Basso et al., 2016, traduction libre : 165). Le principal enjeu soulevé dans la littérature est celui de l'anonymisation des données. L'expression désigne un ensemble de techniques qui ont pour but de « supprimer [les identifiants] personnel des données » et d'ainsi prévenir que d'autres acteurs puissent identifier de nouveau les individus suite au partage de leurs données (Basso et al., 2016, traduction libre : 164). Cet ensemble de techniques se veut un moyen de préserver la vie privée des individus tout en permettant d'extraire des informations précieuses des données de ceux-ci (Basso, et al., 2016). Cependant, comme le pointent Basso et al. (2016, traduction libre : 164) « la sélection et l'application de ces techniques n'est pas une tâche très simple […] dans le contexte [du Big Data] » et le choix d'une technique d'anonymisation inappropriée peut mener à la réidentification des individus et compromettre leur vie privée (Basso, et al., 2016, traduction libre : 164).

La littérature abonde de doutes à l'égard de l'efficacité de ces techniques ainsi que d'exemples prouvant leur faillibilité (Basso et al., 2016; Barocas et Nissenbaum, 2014). Effectivement, Basso et al. (2016) rapportent la réidentification relativement facile et rapide d'une partie des données de près de 500 000 utilisateurs divulguées publiquement par Netflix en seulement 16 jours par des chercheurs d'une université américaine. Cette vulnérabilité considérable rend les organisations

particulièrement susceptibles de subir des attaques de réidentification qui compromettent la sécurité et la vie privée des utilisateurs (Barocas et Nissenbaum, 2014). Malgré les efforts d'experts, les solutions pour contrer ces faiblesses ne sont pas universelles et tardent à être déployées (Basso et al., 2016; Barocas et Nissenbaum, 2014).

Pour leur part, Barocas et Nissenbaum (2014, traduction libre : 55) soulignent que le Big Data et l'analytique des données massives remettent en perspective « l'intuition fondamentale [selon laquelle] l'identité est la plus grande source de préjudice potentiel ». Les auteurs mentionnent que « même lorsque les individus ne sont pas identifiables, ils peuvent être accessibles, peuvent être représentés de manière compréhensible dans des documents qui détaillent leurs attributs et leurs activités, et peuvent faire l'objet d'inférences et de prédictions conséquentes sur cette base » (Barocas et Nissenbaum, 2016, traduction libre : 50). Les données n'ont donc nullement besoin d'être liées à un identifiant personnel pour causer des torts, au contraire. Effectivement, « les entreprises n'auraient aucun intérêt particulier à connaître l'identité d'une personne [puisque] leur capacité à adapter leurs offres et services aux particuliers n'est nullement limitée par l'absence de telles informations » (Barocas et Nissenbaum, 2016, traduction libre : 54). Barocas et Nissenbaum (2014) soutiennent que l'anonymisation des données ne constitue en rien une solution aux enjeux éthiques relatifs à la vie privée et soulignent qu'à la lumière des risques que portent les données non-personnelles, il serait peut-être pertinent de songer les munir d'une protection à la hauteur des dommages qu'elles peuvent causer.

2.2.5 L'analytique des données et enjeux méthodologiques

Comme mentionné plus haut, une partie considérable des enjeux reliés à l'industrie du Big Data provient de l'analytique des données. À cet effet, Breidbach et Maglio (2020) mentionnent de nombreux aspects problématiques méritant une attention particulière. Effectivement, les deux auteurs soulignent le fait que les algorithmes utilisés pour prendre des décisions se basent sur des corrélations et non des relations de cause-à-effet qui établissent un lien sans équivoque entre deux variables (Breidbach et Maglio, 2020; Breidbach et al., 2019; Someh et al., 2019). Breidbach et al. (2019, traduction libre : 669) ajoutent que ces algorithmes sont entraînés à l'aide de « données historiques et souvent subjectives », ce qui empêche la garantie que les décisions prises à l'égard d'individus soient appropriées et éthiques (Boyd et Crawford, 2012; Someh et al., 2019). Ces

multiples inquiétudes nous invitent à examiner la question de plus près, en débutant par la qualité des données utilisées pour entraîner les algorithmes, facteur clé de leur performance et de la valeur de leurs prédictions (Breidbach et Maglio, 2020; Someh et al., 2019).

La qualité des données

La qualité des données peut être lourdement affectée par de nombreux facteurs, notamment la fusion de banques de données de multiples sources et formats (Breidbach et al., 2020; Hand, 2018; Someh et al., 2019), la méthode de collecte, la quantité de données imputées ou encore les différents biais qui sont reflétés dans celles-ci (Martin, 2015). Hand (2018) nous dit également que la qualité des données est définie en fonction des objectifs, qu'elle peut donc être satisfaisante pour répondre à certaines questions, mais moins pour répondre à d'autres, et qu'elle peut se détériorer avec le temps, notamment si les données ne sont pas mises à jour assez régulièrement pour demeurer représentatives du phénomène à l'étude. De leur côté, Someh et al. (2019, traduction libre : 728) soulignent que « les critères de qualité des données pour les systèmes traditionnels ne s'appliquent pas nécessairement » aux données massives et que l'industrie manque de direction à cet égard. Les auteurs soulèvent également des problèmes relatifs à l'agrégation des données qui, outre le fait qu'elle puisse compromettre l'anonymat des individus (Zuboff, 2015), peut faussement représenter ces derniers (Boyd et Crawford, 2012). Finalement, les auteurs appuient le point de Boyd et Crawford (2012) qui souligne l'importance du contexte pour faire parler les données. Effectivement, ces dernières nous disent que les « données [sont] été générées dans des espaces très sensibles au contexte » et que ces éléments contextuels sont importants à analyser pour faire sens des données (Boyd et Crawford, 2012, traduction libre : 673). Les lacunes au niveau de la définition et du maintien des métadonnées risquent de faire perdre la signification réelle des données à travers le partage de celles-ci (Hand, 2018; Someh et al, 2019; Boyd et Crawford, 2012). Le danger est donc de faire dire aux données des choses qu'elles n'ont jamais voulu dire, d'en arriver à des conclusions erronées à propos des individus qu'elles concernent et de prendre des décisions aux retombées potentiellement importantes sur la base d'informations inexactes parce que « l'analytique des données massives [produit des inférences] » qui sont tout sauf des faits absolus (Someh et al., 2019, traduction libre : 728 ; Boyd et Crawford, 2012).

Les biais méthodologiques

Ekbia et al. (2015, traduction libre : 1530) soulignent que « bon nombre des questions méthodologiques qui se posent découlent du stade auquel la subjectivité est introduite dans le processus : c'est-à-dire les décisions prises en termes d'échantillonnage, de nettoyage et d'analyse statistique ». Les données ne parleraient donc pas d'elles-mêmes, bien au contraire (Boyd et Crawford, 2012; Ekbia et al. 2015). Certaines décisions, notamment concernant « les attributs et les variables à conserver, ainsi que celles à ignorer » prises à l'étape du nettoyage des données relèvent du jugement et de l'opinion qui sont profondément subjectifs par nature (Ekbia et al., 2015, traduction libre : 1531).

Boyd et Crawford (2012) mentionnent que toutes les interprétations des données ne sont pas appropriées. Effectivement, il est impératif de poser les bonnes questions aux bonnes banques de données ainsi que d'utiliser la bonne méthode pour y répondre (Hand, 2018). Aussi, tous les échantillons ne sont pas représentatifs de la population en général et utiliser le mauvais échantillon pour répondre à une question peut engendrer des conséquences importantes pour des groupes souvent déjà marginalisés (Boyd et Crawford, 2012). Au sujet des banques de données, Boyd et Crawford (2012, traduction libre : 668) soulignent que la taille de celles-ci offre un terrain particulièrement fertile pour trouver plus de relations statistiquement significatives qu'il n'y en a réellement, « simplement parce que d'énormes quantités de données peuvent offrir des connexions qui vont dans toutes les directions ». Ekbia et al. (2015) mentionnent également les pratiques de *data dredging* et de *cherry picking* qui influencent le processus de façon à générer des résultats qui confirment une position particulière, impactant lourdement leur fiabilité ainsi que le caractère éthique des décisions qui en sont dérivées. Pour leur part, Newell et Marabelli (2015) déplorent le fait que la valeur prédictive d'un algorithme soit considérée comme suffisante alors que les relations qui sous-tendent les prédictions demeurent inconnues. Crawford et al. (2014, traduction libre : 1667) ajoutent que « les actions individuelles agrégées ne peuvent pas, à elles seules, illustrer la dynamique complexe que produit l'interaction [et que] la société est plus grande que la somme de ses parties ». Ekbia et al. (2015 : 1530) résument ces propos en soulignant que « *Big Data seems to be content with the prediction of appearances alone* », ce qui est susceptible de

créer de nombreux enjeux, notamment lorsque personne n'est en mesure d'expliquer le raisonnement d'un algorithme qui rend une décision discriminatoire (Newell et Marabelli, 2015).

Ekbia et al. (2019, traduction libre : 1533) mentionnent les différentes décisions arbitraires prises lors de la cartographie et la représentation graphique des données comme offrant souvent de lourds compromis entre l'« esthétisme et la valeur informative » du message véhiculé. Boyd et Crawford (2012, traduction libre : 670) soulignent de façon éloquente que « la capacité de représenter les relations entre [deux variables] sous forme de graphique ne signifie pas que [le phénomène et sa représentation graphique] transmettent des informations équivalentes ». À cet effet, Hand (2018, traduction libre : 186) nous rappelle « qu'au mieux, un modèle est nécessairement une simplification et une abstraction, le monde étant toujours plus compliqué, souvent de façon insoupçonnée. La fiabilité dépend de la véracité du modèle en tant que représentation des aspects pertinents du monde ». À cela, Boyd et Crawford (2012, traduction libre : 670) ajoutent que les données sont souvent « réduites à ce qui [est adapté] au modèle » altérant donc la signification et la valeur des données d'origine (Crawford et al., 2014). Si ce genre de compromis n'est pas nouveau ou encore exclusif à la science des données, il demeure que « [ces compromis] ne sont pas nécessairement évidents ou encore divulgués [à ceux] qui visualisent les données » (Ekbia et al., 2015, traduction libre : 1533).

Identité digitale et réalité

L'analytique des données massives offre la possibilité aux organisations de cibler de façon très précise les individus et de prédire leurs comportements sur la base « des détails quotidiens de leur vie » (Newell et Marabelli, 2015, traduction libre : 3; Someh et al., 2019). Les prédictions de contenu approprié sont faites sur la base de données historiques agrégées comme « les comportements passés, la localisation, l'âge et le genre » des utilisateurs, mais surtout, se basent sur la prémisse incertaine que ces données les représentent réellement (Someh et al., 2019, traduction libre : 726; Boyd et Crawford, 2012). Effectivement, ces « profils digitaux » sont constitués d'une panoplie de données d'origines diverses, dont certaines sont issues de médias sociaux (Breidbach et al., 2019, traduction libre : 670; Someh et al., 2019). Certains auteurs avancent le fait que ces données représentent davantage ce que les gens veulent projeter comme

image, plus que ce qu'ils ne sont réellement (Hand, 2018; Boyd et Crawford, 2012). Contrairement à ces dernières, les « données administratives » issues d'un suivi qui échappe aux intentions des utilisateurs, comme celles récoltées à travers l'internet des objets (Breidbach et al. 2019) « révèlent énormément sur ce que les gens font, avec qui ils interagissent, […] leurs intérêts et même leurs croyances [et] nous rapprochent de la réalité sociale » selon Hand (2018, traduction libre : 180; Breidbach et al. 2019). Boyd et Crawford (2012) appellent à la vigilance dans l'interprétation de ces données qui sont loin d'être équivalentes à la réalité, surtout si prises hors contexte. Someh et al. (2019) déplorent que ces profils qui décrivent parfois de façon inexacte les individus soient, malgré tout, utilisés pour baser des prédictions et prendre des décisions à leur égard qui peuvent être inappropriées, injustes et discriminatoires.

Biais et discrimination dans l'exploitation des données

Boyd et Crawford (2012) pour leur part renchérissent sur la question des biais intégrés aux données et aux algorithmes et attaquent les affirmations d'objectivité faites par l'industrie du Big Data. Effectivement, elles démentent ces dernières en nous rappelant la subjectivité inhérente à toute méthodologie, y compris en science des données. Richterich (2018, traduction libre : 49) abonde en ce sens et ajoute que « l'intérêt d'une entreprise dans la création de données est la principale source de biais » puisqu'il oriente inévitablement et teinte de subjectivité toutes les étapes de la mise en œuvre (Ekbia et al. 2015). Boyd et Crawford (2012, traduction libre : 667) relatent l'ironie derrière les affirmations d'objectivité du Big Data en soulevant le fait que « [ces] prétentions d'objectivité sont nécessairement formulées par des [individus] et […] fondées sur des observations et des choix subjectifs ».

Maintenant, cette subjectivité est la source de nombreux biais qui sont susceptibles d'être intégrés aux algorithmes dès leur conception (Boyd et Crawford, 2012). L'entraînement de ces algorithmes sur des données reflétant injustices et inégalités à l'égard de certaines populations et individus accentue davantage les risques que ces derniers rendent des décisions discriminatoires qui perpétuent des « préjugés institutionnalisés » (Martin, 2015, traduction libre : 73; Boyd et Crawford, 2012; Hand, 2018). Une autre conséquence possible du processus de décision algorithmique est ce que Breidbach et Maglio (2020, traduction libre) appellent la « discrimination par procuration ». Des éléments aux apparences inoffensives, comme le code postal d'un individu,

deviennent alors des vecteurs de discrimination dissimulés par l'opacité et l'autonomie du processus (Breidbach et Maglio, 2020).

Newell et Marabelli (2015) notent que si les organisations ont toujours eu recours à la discrimination pour offrir leurs produits et services aux publics appropriés, l'ère du Big Data, de l'analytique et des décisions algorithmiques leur permettent de repousser les limites du possible. Effectivement, les organisations utilisent les tendances et les courants qui émanent des données massives pour catégoriser les individus et prendre des décisions à leur égard (Newell et Marabelli, 2015). Les auteurs prennent en exemple le cas des hommes qui se font accabler de primes d'assurances automobiles faramineuses sous le prétexte qu'ils ont, en tant que groupe, une conduite plus dangereuse que celle des femmes. Cette pratique a été reconnue discriminatoire sur le territoire de l'Union européenne, puisqu'en effet, si cette tendance est bel et bien observée, conclure que tous les hommes y correspondent sans égard à leurs réels comportements d'automobiliste n'est pas juste (Newell et Marabelli, 2015). Richterich (2018) note les biais de sélection qui peuvent émaner de ces tendances dérivées de données massives. Effectivement, ces données peuvent ne représenter qu'une petite partie de la population, celle qui est jeune, active sur les réseaux sociaux et à l'affût des nouvelles technologies par exemple, et donc en exclure la majorité (Richterich, 2018). Le danger réside dans la possibilité que les conclusions dérivées de ces données reflètent les valeurs d'une population relativement homogène et écartent celles des autres populations, ou encore qu'elles servent à prendre des décisions à l'égard d'individus qui ne sont pas représentés de façon appropriée par un échantillon, menant à de potentielles discriminations et iniquités (Richterich, 2018; Hand, 2018; Crawford et al., 2014).

2.3 Enjeux éthiques liés au développement et à l'implantation de systèmes d'intelligence artificielle mobilisant l'informatique affective

Avant d'enchaîner sur les enjeux soulevés par les technologies d'informatique affective, il convient de prendre le temps de bien définir ce champ d'étude ainsi que la science de laquelle il découle : l'intelligence artificielle.

Le domaine de l'intelligence artificielle, dont l'origine remonte au milieu des années 1900 a d'abord été défini comme « la science et l'ingénierie de la fabrication de machines intelligentes »

(McCarthy, 2007, cité de Ostrom et al., 2019, traduction libre : 80). Cependant, les différentes définitions données au domaine aujourd'hui ne font pas consensus (Ostrom et al.,2019). Effectivement, l'IA peut être simplement définie comme étant toutes formes d'« intelligence non-biologique » (Tegmark, 2017, cité de Ostrom et al., 2019, traduction libre : 80) ou encore « une intelligence affichée ou simulée par des […] algorithmes ou des machines » (Coeckelbergh, 2020, traduction libre : 64). L'IA comporte deux branches d'applications et de recherches dont la deuxième est d'une importance particulière pour ce rapport. La première, l'IA générale, désigne la capacité d'accomplir n'importe quelle tâche, de généraliser l'intelligence de la machine à toutes les sphères, ce qui contraste avec la deuxième branche, l'IA faible, destinée à accomplir des tâches spécifiques et limitées (Ostrom et al., 2019; Coeckelbergh, 2020). Comme le souligne Coeckelbergh (2020, traduction libre : 67) « l'IA peut être définie à la fois comme une science et une technologie ». Effectivement, en tant que science elle nous permet de développer les connaissances et d'atteindre une meilleure compréhension de l'être humain (Coeckelbergh, 2020). L'IA est également une technologie qui prend différentes formes, comme des *chatbots* ou encore des montres intelligentes, qui ont pour but d'accomplir des tâches concrètes et spécifiques (Coeckelbergh, 2020). Ces technologies sont propulsées par des algorithmes qui s'alimentent des données de l'environnement pour fournir des prédictions (Coeckelbergh, 2020). En fait, c'est dans ces algorithmes que réside la « base de leur intelligence » (Coeckelbergh, 2020, traduction libre : 70).

L'informatique affective est un sous-domaine de l'intelligence artificielle qui, comme mentionné dans l'introduction de cette revue de littérature, s'intéresse aux émotions (McStay, 2020). Plus précisément, l'informatique affective est une forme d'IA faible qui « englobe à la fois la création et l'interaction [de l'humain] avec des systèmes de machines qui détectent, reconnaissent, répondent et influencent [ses] émotions » (Daily, James, Cherry, Porter III, Darnell, Isaac et al., 2017, traduction libre : 213; McStay et Urquhart, 2019). Pour réussir à traduire « la vie émotionnelle [d'une façon qui soit] lisible par les machines » (McStay et Urquhart, 2019, traduction libre), les technologies d'informatique affective dépendent de données particulières que Landowska (2019, traduction libre : 275) appelle des « symptômes d'émotions ». Ces données sont captées à l'aide de canaux adaptés à la ou les sources dont elles proviennent pouvant varier de l'expression faciale, la posture du corps, des patrons comportementaux, des caractéristiques de la

prosodie et de textes écrits, ou encore de caractéristiques physiologiques comme le rythme cardiaque, la température du corps, la respiration et la réponse galvanique de la peau, par exemple (Landowska, 2019; McStay et Urquhart, 2019).

Le domaine a été développé sur la prémisse que « pour que les ordinateurs soient intelligents et interagissent naturellement avec les humains dans des situations du monde réel, ils doivent être capables de reconnaître et d'exprimer des émotions » (Richardson, 2020, traduction libre : 77). Aujourd'hui, les intérêts de l'industrie pour cette technologie varient grandement (McStay et Urquhart, 2019). Effectivement, les capacités de l'informatique affective sont mises à profits dans différents domaines, comme l'analytique média, la santé, l'éducation et la sécurité par exemple (Daily et al., 2017; McStay, 2020). Effectivement, certaines organisations utilisent l'information que transmettent les expressions faciales pour analyser et améliorer la performance de leur contenu numérique, alors que d'autres s'en servent pour fournir du contenu personnalisé déterminé sur la base du profil émotionnel de leurs utilisateurs (McStay, 2016). Des organisations s'en servent en milieu organisationnel pour analyser les dynamiques de groupe et la productivité, alors que d'autres en font usage dans le domaine de la santé et le bien-être psychologique en aidant leurs utilisateurs à détecter des signaux déclencheurs, prévenir des crises et réguler leurs émotions (Daily et al., 2017; McStay, 2020).

Malgré les diverses finalités pour lesquelles elles sont exploitées, l'attrait principal de ces technologies demeure le même peu importe leur domaine d'application. Effectivement, elles permettent à toutes les organisations qui les détiennent de jeter un coup d'œil dans l'esprit des utilisateurs et d'en extraire des informations précieuses « que les mots [à eux] seuls ne pourraient jamais » révéler (Feldman Barrett et al., 2019; McStay et Urquhart, 2019**;** Yonck, 2020, traduction libre : VIII).

La présente section portera sur les enjeux méthodologiques et éthiques que portent les technologies d'informatique affective. Nous adresserons les prémisses sur lesquelles les technologies s'appuient ainsi que leurs limitent, leurs implications pour la prise décisions algorithmiques, les risques de manipulation affective que ces technologies portent ainsi que l'impact de leur déploiement dans la sphère publique.

2.3.1 Enjeux méthodologiques des technologies affectives

Les technologies d'informatique affective s'attirent de nombreuses critiques en raison de leurs enjeux méthodologiques. Des inquiétudes relatives « au manque de considération accordée aux émotions culturelles » ont été soulevées, particulièrement en ce qui a trait à la reconnaissance des émotions à travers les expressions faciales (Brigham, 2017, traduction libre : 403). Des auteurs notent l'importance du contexte socio-culturel dans l'apprentissage des émotions et la variabilité susceptible d'être observée d'une culture à l'autre en ce qui a trait à ce qui est approprié ou non ou encore à quand il est approprié d'exprimer une émotion (Brigham, 2017). Cette variabilité s'étendrait également à la façon dont les individus réagissent dans différents contextes, ce qui est susceptible de varier grandement d'un individu à l'autre (Bullington, 2005). Cependant, bon nombre des algorithmes de vision artificielle sont entraînés sur le système FACS de Paul Ekman qui se base sur la prémisse qu'il existe des « émotions universelles de base révélées par les mouvements des muscles faciaux de la même façon à travers l'âge, le genre, l'origine ethnique et la culture » (Richardson, 2020, traduction libre : 82). Cette prémisse rendrait le système FACS trop homogène et donc, « peu fiable, inclusif et utile » pour une grande partie de la population (Brigham, 2017, traduction libre : 403 ; McStay, 2016). Effectivement, l'opinion commune qui fait référence à l'hypothèse de Paul Ekman est controversée (Feldman Barrett et al., 2019). Effectivement, les évidences dégagées d'une méta analyse conduite par plusieurs chercheurs suggèrent beaucoup plus de variabilité dans l'expression des émotions entre cultures, d'une personne à l'autre et d'une situation à l'autre que ce que l'opinion commune laisse entendre. Sans être complètement dénuée d'informations sur les états émotionnels, l'expression faciale d'un individu serait loin d'en constituer leur expression fiable. Selon les auteurs de la méta analyse, il serait impossible « de déduire avec certitude qu'un sourire indique [la joie ou encore] qu'un froncement de sourcils indique la tristesse » (Feldman Barrett et al., 2019, traduction libre : 46).

Landowska (2019, traduction libre : 274-275) pour sa part nous dit que la reconnaissance des émotions automatique mesure un « phénomène humain interne et complexe » sur la base de « symptômes d'émotions externes ». Elle produit donc, tout au plus, une estimation sujette à de nombreuses erreurs (Landowska, 2019). Effectivement, l'auteure souligne de nombreux éléments pouvant affecter les résultats et l'applicabilité des solutions de reconnaissance des émotions à

travers les expressions faciales. Par exemple, elle mentionne que l'environnement physique peut entraver la captation des images et exprime les risques d'erreur associés à l'utilisation d'un seul type de données en comparaison avec un système multimodal (Landowska, 2019; Richardson, 2020).

Ces enjeux méthodologiques, tout comme ceux présentés dans la section précédente, ont des implications considérables pour la prise de décision algorithmique. Les algorithmes à la base des technologies d'intelligence artificielle produisent des prédictions qui forment la base de décisions (Coeckelbergh, 2020). Ces algorithmes sont souvent issus du sous-domaine de l'apprentissage machine parfois qualifiée de « boîte noire » en raison de l'opacité de son processus (Coeckelbergh, 2020). Effectivement, « si les programmeurs connaissent l'architecture du réseau, [ils] ne savent pas exactement ce qui se passe [entre l'entrée et la sortie] et donc comment [les algorithmes] arrivent à [leurs] décisions » (Coeckelbergh, 2020, traduction libre : 72). Un aspect problématique est que ces algorithmes prennent souvent ces décisions de façon complétement autonome et ne requièrent que très rarement le jugement humain (Breidbach et Maglio, 2020). Lorsque celui-ci est requis, l'opacité du processus et la représentation graphique des résultats obscurcissent les différents compromis, limitations et enjeux de qualité soulevés plus haut et entravent la capacité de l'humain à bien interpréter ou encore de contester les résultats présentés (Ekbia et al., 2015; Breidbach et al., 2019). Cette incompréhension du processus de décision algorithmique « entièrement transféré au domaine technique » souligne le manque d'implication humaine, complique la notion d'imputabilité et empêche d'assurer hors de tout doute le caractère éthique des décisions prises (Breidbach et Maglio, 2020, traduction libre; Breidbach et al., 2019). Les critiques relatives aux prémisses de base sur laquelle se fondent les algorithmes d'informatique affective remet également en doute le caractère éthique des décisions que ceux-ci peuvent prendre (McStay et Urquhart, 2019). Effectivement, McStay et Urquhart (2019) soulignent le manque de preuve causale entre l'expression faciale et la présence d'une émotion comme une entrave profonde à la prise de décision algorithmique qui peut entraîner des injustices et un traitement discriminatoire des individus.

L'incertitude à l'égard de la fiabilité des résultats offerts par les technologies d'informatique affective nécessite également de porter une attention particulière à la façon dont la technologie est

représentée. Effectivement, à la lumière des résultats présentés ci-haut, il serait trompeur d'utiliser des termes comme « expression émotionnelle » (Feldman Barrett et al., 2019) qui peuvent laisser croire à l'utilisateur que les résultats sont sans équivoque et sans nuances (Cowie, 2012). À cet effet, Landowska (2019) ajoute qu'il serait parfois plus juste d'exprimer cette incertitude explicitement que de fournir des résultats incertains sans même divulguer le niveau de confiance associé, surtout dans la mesure où ces solutions peuvent servir à prendre des décisions à l'égard des individus (Richardson, 2020). Cowie (2012, traduction libre : 419) nous dit que cette transparence est nécessaire alors que « peu de gens comprennent ce que l'on peut et ne peut pas attendre [de la part] d'une machine ». Effectivement, l'auteur souligne que les utilisateurs des technologies ne possèdent pas les connaissances nécessaires pour les comprendre et développer des attentes adéquates face à leurs capacités. Les risques sont donc que, par leur mauvaise interprétation de la technologie, les utilisateurs en viennent à se fier à celle-ci d'une façon inappropriée et qui pourrait leur causer du tort (Cowie, 2012). Effectivement, ces torts sont particulièrement évidents alors que de plus en plus de robots sociaux dotés de systèmes de reconnaissance des émotions intègrent nos vies. Scheutz (2012, traduction libre) déplore la tendance des organisations à présenter ces technologies d'une façon qui les personnifie, malgré le fait que « leurs limites computationnelles et cognitives » soient connues. Ces descriptions trompeuses quant aux réelles capacités des technologies sont susceptibles de faire croire au public que leurs compagnons vivent les émotions qu'ils affichent alors que ce n'est pas le cas (Scheutz, 2012; Cowie, 2012; Picard et Klein, 2002). Cowie (2012, traduction libre : 420) souligne le principe de « pars pro toto » qui désigne la difficulté pour l'être humain « de ne pas déduire que, si un système présente des fragments de comportements étonnamment humains, il en possède d'autres […] qui [sont habituellement] associés à ces [comportements] chez un humain ». Sullins (2012, traduction libre : 408) souligne que de jouer avec cette prédisposition constituerait « un manque de respect à l'égard de l'agence humaine », surtout considérant le peu de connaissances dont le public détient pour se représenter la technologie autrement (Cowie, 2012).

2.3.2 Machines et humanité

Par la nature sensible des informations qu'elles traitent, les technologies d'informatique affective poussent la question de la manipulation encore plus loin. Effectivement, à quel point sommes-nous confortables avec le fait que ces systèmes puissent interférer avec notre vécu émotionnel (Daily et

al., 2017) ? Certains sont d'avis que les dangers ne sont pas tant reliés à la manipulation elle-même, dans la mesure où il est possible qu'elle soit motivée par de bonnes intentions et qu'elle n'ait aucune conséquence néfaste, voire au contraire (Picard et Klein, 2002). Les dangers seraient donc davantage liés aux fins visées par la manipulation (Cowie, 2012) qui peuvent rapidement compromettre « l'intégrité personnelle » des utilisateurs (Duffy, 2008). À cet effet, Daily et al., (2017, traduction libre : 225) nous disent qu'il faut faire attention de ne pas « permettre à ces machines affectives d'affecter négativement les humeurs positives, de limiter les sentiments des utilisateurs ou encore d'entraver leur vie privée mentale et émotionnelle ». Une technologie « particulièrement disposée » à la manipulation émotionnelle est l'INAD (Steinert et Friedrich, 2020). Effectivement, vu le rôle important que jouent les émotions dans la prise de décision, la manipulation émotive s'avère une arme incroyable pour les organisations. Plus particulièrement, le profil émotionnel des utilisateurs aiderait les organisations à cibler le contenu le plus susceptible de les pousser à adopter le comportement souhaité, stratégie qui comporte son lot de considérations éthiques à l'égard de « l'intégrité mentale et [de] la liberté cognitive » des utilisateurs (Steinert et Friedrich, 2020, traduction libre : 359 ; McStay et Urquahart, 2019).

Le domaine de l'informatique affective implique également la possibilité que de plus en plus de robots sociaux avec lesquels nous bâtirons des relations intègrent nos vies. Partant du raisonnement « pars pro toto » mentionné plus haut (Cowie, 2012), les capacités émotionnelles actuelles des robots, limitées à la simulation des émotions, peuvent facilement mener à l'attribution de capacités qui ne sont pas réelles ainsi qu'au développement de relations trompeuses (Picard et Klein, 2002; Duffy, 2008; Beavers et Slattery 2017). Effectivement, les risques sont qu'à travers le développement d'une relation faussement bidirectionnelle avec la machine, l'utilisateur oublie qu'elle est incapable de réciprocité et forme des attentes envers celle-ci qu'elle ne peut rencontrer (Scheutz, 2012; Duffy 2008; Cowie, 2015). Ces relations trompeuses et unidirectionnelles peuvent mener à des dépendances psychologiques et affectives qui placent l'humain dans une position particulièrement favorable à l'exploitation et la manipulation (Scheutz, 2012; Duffy, 2008). La possibilité existe que des robots soient conçus à des fins de tromperie et que les expressions qu'ils affichent dissimulent des intentions malhonnêtes (Cowie, 2015). À cet effet, Scheutz (2012, traduction libre) soulève les risques que le robot puisse profiter de cette relation de dépendance ainsi que de la confiance que l'humain lui confère pour le persuader de « commettre des actions

qu'il n'aurait jamais commises autrement » pouvant servir aux fins économiques d'une organisation par exemple (Cowie, 2015).

De leur côté, Daily et al., (2017) contemplent la possibilité que l'informatique affective puisse donner naissance à des agents moraux utilisés pour aider l'humain à naviguer son vécu émotionnel. Les auteurs s'inquiètent des effets potentiellement néfastes que la dépendance à ces robots pourrait avoir sur les habiletés émotionnelles des enfants, ainsi que sur la capacité des adultes à gérer leurs émotions de façon indépendante. Sur le même ordre d'idée, Beavers et Slattery (2017) soulignent la possibilité que l'informatique affective puisse affecter l'intelligence émotionnelle des individus. Effectivement, les auteurs s'inquiètent que les technologies qui exploitent ce domaine puissent induire une certaine « confusion face à nos propres états affectifs et interfèrent avec notre capacité à comprendre les états affectifs des autres » (Beavers et Slattery, 2017, traduction libre : 24).

Un autre enjeu important est celui de l'impact potentiel des technologies d'informatique affective sur l'identité humaine (McStay et Urquhart, 2019; Steinert et Friedrich, 2020). Par exemple, McStay et Urquhart (2019, traduction libre) soulignent qu' « en rendant l'émotion visible, [les technologies d'informatique affective] peuvent avoir un impact sur l'espace laissé aux individus pour formuler leurs propres idées et identités ». Les auteurs s'inquiètent du rôle de plus en plus important que prennent ces technologies dans « la [co-construction] des perceptions et de la compréhension des émotions », alors que ces dernières servent souvent les intérêts d'organisations dont les intentions ne sont pas toujours louables (McStay et Urquhart, 2019, traduction libre). Steinert et Friedrich (2020) sont d'un avis similaire et soulignent que les INAD pourraient avoir des implications considérables pour les habiletés émotionnelles des utilisateurs et interférer avec leur identité. Effectivement, l'autonomie de fonctionnement d'un système qui opère le suivi constant des états affectifs de l'utilisateur « pourrait compromettre [sa] capacité de réfléchir à [ces derniers] et de délibérer à savoir s'il veut agir [sur ceux-ci] […], [alors que cette] capacité est une composante cruciale [de] [l'agence] morale » (Steinert et Friedrich, 2020, traduction libre : 358). La capacité de la technologie d'influencer et de simuler des états affectifs révèle la possibilité qu'une grande partie de l'univers émotionnel de l'utilisateur puisse être déléguée à la machine. Effectivement, elle pourrait interférer avec la notion de responsabilité à l'égard de ses émotions, compromettre ses capacités de régulation émotionnelle ainsi que brouiller la distinction entre ses

émotions propres et celles qu'elle génère. Ces éventualités potentielles sont profondément troublantes et pourraient remettre en question ce que signifie être humain (Steinert et Friedrich, 2020).

Finalement, Cowie (2015) exprime les risques des technologies d'informatique affective pour l'autonomie humaine. Effectivement, l'auteur explique que pour exercer son autonomie, l'individu « doit être à l'abri des facteurs qui compromettent ou sapent [sa] capacité à se remettre en question et à décider de manière rationnelle », ce que les différentes applications de la technologie peuvent entraver (Cowie, 2015, traduction libre). De façon intéressante, il souligne également que les informations émotionnelles peuvent elles-mêmes constituer un facteur compromettant cette capacité puisque « si elles deviennent disponibles », comme l'ont noté McStay et Urquhart (2019) plus haut, « elles peuvent restreindre [les options de l'individu] d'une manière qu'il ne choisirait pas » (Cowie, 2015, traduction libre).

2.3.3 Surveillance affective

Les problèmes méthodologiques mentionnés plus haut, dont l'industrie est pleinement consciente, soulignent la nécessité d'une approche plus complète et hybride qui combine les contextes internes, externes et sociaux propres à l'individu (McStay et Urquhart, 2019). Cependant, comme l'indiquent McStay et Urquhart (2019), la prise en compte du contexte implique nécessairement davantage de données qui, elles, devront être collectées par divers moyens, et ce, dans toutes les sphères de la vie. Cette nouvelle approche nécessiterait donc un déploiement grand échelle dans les espaces privés comme publics, ce qui n'est évidemment pas sans implications pour la vie privée des individus (McStay et Urquhart, 2019).

McStay et Urquhart (2019, traduction libre) soulignent que l'omniprésence de technologies qui « rendent visibles […] les états affectifs » des individus dans les infrastructures des espaces publics rendra difficile pour ces derniers de « résister à l'observation et la surveillance ». Fait intéressant, ces derniers mentionnent que l'approche hybride et multimodale de collectes de données émotionnelles susceptible d'émerger suite aux nombreuses critiques méthodologiques mentionnées plus haut risque de signifier que des informations personnelles seront nécessairement traitées conjointement avec ces dernières. Cette éventualité voudrait donc dire que les

organisations derrières ces technologies seraient assujetties aux régulations sur la protection des données personnelles, comme le RGPD. Néanmoins, l'approche ambiante comporte son lot de questions puisque l'applicabilité de ces régulations dans les espaces publics est particulièrement complexe (McStay et Urquhart, 2019).

Effectivement, les auteurs soulignent que les espaces publics sont composés « d'un assemblage complexe d'acteurs » qui peuvent être inconnus des individus et avec qui ces derniers n'ont pas nécessairement de « liens contractuels » formels (McStay et Urquhart, 2019, traduction libre). Ils ajoutent que les attentes en termes de respect de la vie privée dans les différents espaces et les obligations des différents acteurs à cet égard ne sont pas claires. Effectivement, ces questions dépendent de nombreux facteurs légaux et d'autant plus complexifiées alors que « de nombreux cas de surveillance de l'espace public impliquent une externalisation ou un partenariat avec des organisations privées » (McStay et Urquhart, 2019).

Les technologies d'informatique affective impliquent la possibilité que la reconnaissance des émotions puisse être utilisée dans les systèmes de surveillance pour inférer « les états psychologiques et les motivations des individus » (Bullington, 2005, traduction libre : 98). En plus de constituer une violation de la vie privée évidente, il a été démontré que la technologie n'est pas exempte d'erreurs (Bullington, 2005; Feldman Barrett et al., 2019; Landowska, 2020). Il est donc très plausible que ces systèmes de surveillance affectifs attribuent des états affectifs et des intentions à des individus qui sont erronés (Bullington, 2005). Comme le soulignent McStay et Urquhart (2019), alors que le RGPD porte son attention exclusivement aux torts causés par l'identification des individus et qu'il ne protège pas l'utilisation des inférences dérivées des données personnelles, il néglige les conséquences potentielles de la surveillance qui peut mener à la catégorisation et le traitement discriminatoires des individus (González Fulter, 2010).

Finalement, les applications d'auto-traçage sont notées comme ayant un potentiel effet normatif sur les individus pouvant porter atteinte à leur autonomie et leur authenticité (Steinert et Friedrich, 2020). Steinert et Friedrich (2020, traduction libre : 358) considèrent la possibilité que les INAD exercent un effet similaire et que leur déploiement puisse générer « des pressions sociales sur les individus d'auto réguler leurs émotions » afin de correspondre à la norme. À la lueur des faits

précédemment mentionnés, il n'est pas irréaliste d'imaginer que ces technologies puissent contribuer à l'effet de contrôle et de régulation de l'industrie du Big Data.

2.4 Conclusion

Dans un premier temps, cette revue de littérature nous a permis de prendre connaissance des impacts de l'industrie sur les individus et la société. Entre autres, nous avons pu constater des acteurs commerciaux tout puissants dont les intérêts financiers poussent à l'adoption de pratiques néfastes qui sont lourdes d'implications pour les droits et libertés des utilisateurs. La deuxième section nous a permis d'aborder les différents enjeux inhérents à la gouvernance des données. Cette section a révélé un consentement souvent bafoué, notamment par des pratiques de partage de données qui, elles, ne font que donner de l'ampleur aux conséquences qui incombent les utilisateurs. Cette section a également fait lumière sur des enjeux méthodologiques importants qui remettent en cause les prétentions d'objectivité de la science des données et nous a permis de constater les nombreuses conséquences potentielles de l'analytique des données. Finalement, nous avons abordé les enjeux spécifiques aux technologies d'informatique affective. À l'instar de la section précédente, celle-ci a révélé de nombreux enjeux méthodologiques qui remettent en cause les fondements mêmes de la science sur laquelle ces technologies s'appuient. La section a également révélé les risques inhérents d'une technologie qui interfère avec nos émotions, une partie intégrante de notre identité et de notre humanité.

La prochaine section nous permettra de sortir de la littérature et d'aller jeter un coup d'œil sur l'environnement organisationnel d'EmoScienS pour voir ce qui s'y passe. Réalisée en deux temps, notre analyse nous permettra d'abord de nous ancrer dans le concret en repérant les mouvements et les tendances que connait l'écosystème de l'IA au pays. Nous irons ensuite à la rencontre des acteurs de l'environnement compétitif de la *startup* pour recenser et comparer les pratiques des gestions des données personnelles que ces derniers adoptent. À l'issu de celle-ci, nous aurons dressé le portrait d'un écosystème mouvementé ainsi que parsemé d'initiatives et de pratiques qui ne sont pas sans rappeler plusieurs des enjeux éthiques soulevés plus haut.

3. ANALYSE DE L'ENVIRONNEMENT ORGANISATIONNEL D'EMOSCIENS

La présente section a pour objectif de présenter un aperçu de l'état actuel de l'écosystème de la *startup*. Réalisée d'une part à l'aide du modèle PESTEL, l'analyse fait ressortir les événements pertinents se déroulant dans les sphères politique, économique, socioculturelle, technologique, environnementale et légale d'EmoScienS. L'analyse qui suit révèle des éléments parfois avantageux, parfois moins, mais tous susceptibles d'influencer et d'orienter EmoScienS dans ses choix stratégiques à court, moyen, et long-terme. Dans une deuxième partie, nous réaliserons une analyse comparative des pratiques éthiques de l'industrie. À travers la sélection d'un petit échantillon de compétiteurs, nous pourrons dresser le portrait des pratiques répandues, éclairant ainsi les opportunités de positionnement concurrentiel.

3.1 Analyse PESTEL

3.1.1 Perspective politique

Stratégie pancanadienne : La stratégie pancanadienne déployée en 2017 par le gouvernement du Canada est considérée insuffisante par les acteurs de l'écosystème de l'IA au pays (Deschamps, 2020). Comme le souligne le rapport « Point critique pour la politique publique » de Deloitte (2019b), « les forces en talents et en recherche du pays ne suffiront pas pour revendiquer le leadership du Canada en IA ». La stratégie que propose le Canada est beaucoup moins exhaustive et transversale que celles des autres pays, comme recensé par l'Institut canadien de recherches avancées dans son rapport « L'ère de l'IA » (Kung, Boskovic et Stix, 2020). Le déséquilibre de notre stratégie risque de désavantager les *startups* et les PME canadiennes sur la scène internationale. Effectivement, la compétition risque d'être particulièrement féroce dans la mesure où les entreprises canadiennes devront tenter de faire leur place sur un marché peuplé d'organisations soutenues par des stratégies nationales beaucoup plus costaudes que la stratégie pancanadienne actuelle.

Absence de politiques encadrant l'IA : Comme souligné par le rapport « Impératif de l'IA : Point critique pour la politique publique » de Deloitte (2019b), le Canada ne possède aucun cadre

législatif ou politique encadrant l'utilisation de l'intelligence artificielle et n'est doté d'aucune stratégie nationale de gestion des données. Les lois canadiennes et provinciales relatives à la protection des données utilisateurs ne sont pas suffisantes pour couvrir l'ensemble des sujets sensibles relevant de l'utilisation de l'intelligence artificielle. Le gouvernement canadien a lancé le Conseil Consultatif en matière d'intelligence artificielle du gouvernement du Canada dont l'une des tâches sera de « contribuer à l'élaboration des politiques gouvernementales dans les domaines liés à l'IA et à l'intégration de l'IA dans divers secteurs » (Innovation, Sciences et Développement Économique Canada, 2019). Il a également procédé à des consultations nationales sur le numérique et les données ayant données naissance à « La Charte numérique du Canada en action » (Innovation, Sciences et Développement Économique Canada, 2019b) qui pourrait déboucher sur une stratégie nationale des données, selon le rapport « Une stratégie des données pour le Canada » publié sur le site du forum des politiques publique (Scassa, 2019). Cette situation place les entreprises d'IA au Canada dans une position d'incertitude opérationnelle dans la mesure où elles doivent naviguer un flou légal et politique susceptible d'être comblé prochainement (Deloitte, 2019b). Ces changements vont certainement affecter les organisations et pourraient désavantager les entreprises dont les capacités financières limitent la marge de manœuvre. La question demeure également à savoir quel niveau de réglementation sera imposé pour à la fois favoriser l'innovation et le développement économique du pays, mais de façon cohérente avec le discours global concernant l'éthique de l'IA et l'importance de la confiance des citoyens.

Crise et instabilité : Le gouvernement canadien est aux prises avec la gestion d'une crise de santé publique engendrée par la pandémie de Covid-19. Sa gestion de la situation a soulevé de nombreuses insatisfactions des partis de l'opposition qui ont beaucoup de poids et d'exigences envers le gouvernement libéral minoritaire actuel. La dette nationale s'accumule et la question du remboursement de ces sommes exorbitantes soulève beaucoup d'inquiétudes et de tensions comme le souligne l'article de La Presse « Le discours du Trône » (2020) qui relate les opinions du public suite à la lecture du discours du trône du gouvernement libéral en septembre dernier. Le gouvernement actuel capitalise beaucoup sur l'avenir des technologies en investissant des sommes considérables dans le domaine de l'innovation et des technologies (Rettino-Parazelli, 2019), mais la précarité de la situation économique actuelle ainsi que l'insatisfaction des Canadiens et autres

parties prenantes pourrait remettre en question l'ampleur de l'aide que le gouvernement apporte à ce sur le long-terme.

3.1.2 Perspective économique

Création d'un nouveau segment économique : Avec la transformation d'une économie de plus en plus digitale, le marché du travail est appelé à changer. Les inquiétudes relatives à la vie privée, à la gestion des données personnelles, à la responsabilité et la transparence, encore majoritairement non traitée par la législation actuelle et les politiques canadiennes, correspondent à un nouveau créneau qui fait tranquillement sa place sur le marché, celui de l'IA responsable. Effectivement, la création du Centre d'expertise internationale de Montréal pour l'avancement de l'intelligence artificielle, le programme IA et Société du CIFAR faisant partie de la stratégie pancanadienne, les cours en ligne, école d'été et programmes d'étude portant de près ou de loin sur l'éthique de l'intelligence artificielle en sont de bons exemples. Ce nouveau marché créera de nouveaux emplois, programmes de formation et intérêts de recherche ainsi que des besoins d'investissements importants. Considérant que l'intérêt pour l'éthique de l'intelligence artificielle est de plus en plus considéré comme un sujet prioritaire et d'importance capitale dans l'agenda d'une majorité de nations, le support apporté à ce nouveau marché devra être considérable. Effectivement, ce nouvel intérêt impactera les nouveaux besoins en termes de compétences mentionnés par le rapport « Point critique pour la politique publique » de Deloitte (2019b). Le document mentionne que l'automatisation de certaines tâches occasionnera la perte des emplois de Canadiens estimée à 40% par le *Brookfield Institute for Innovation and Entrepreneurship* (Deloitte, 2019b). Ces pertes nécessiteront le déplacement des compétences vers les secteurs porteurs de croissance de cette nouvelle économie digitale, desquels le domaine de l'éthique de l'IA fait sans doute partie.

Incertitude économique et PME : Le contexte d'incertitude économique actuel est peu propice à la dépense pour les PME qui, à elles seules, représentent 90% des entreprises au pays (Gouvernement du Canada, 2019). Effectivement, depuis le début de la pandémie, les ventes des entreprises ont drastiquement chuté, le taux d'endettement des PME a augmenté tout comme le coût des primes d'assurance qui les incombe en raison des risques associés à la pandémie (Giguère, 2020). Le fardeau financier s'alourdit pour les organisations dont l'objectif premier en ces temps

difficiles demeure de pouvoir s'acquitter de leurs frais fixes et dépenses essentielles pour, au minimum, garder la tête hors de l'eau (Normand, 2020). L'incertitude et la possibilité de confinement qui risquent de perdurer laissent présager le maintien de cette situation financière précaire à moyen terme pour la majorité d'entre elles, pouvant affecter une partie de la clientèle potentielle d'EmoScienS.

3.1.3 Perspective socioculturelle

Santé mentale au Québec : Nous assistons à un cri du cœur de la population québécoise en ce qui a trait à la santé mentale. Effectivement, comme nous l'a démontré l'étude sur la santé psychologique des étudiants de l'Université de Montréal menée par la FAÉCUM il y a quelques années (Lessard, 2016), la situation était déjà inquiétante au Québec. Les enjeux de santé mentales ne sont qu'aggravés par la pandémie actuelle qui plonge la population dans l'isolement, l'anxiété et l'épuisement (Lauzon, 2020). Malgré ses investissements tardifs (Crête, 2020), le gouvernement du Québec est accusé de ne pas avoir su livrer la marchandise à temps et prévoir des mesures pour éviter ce qui est aujourd'hui considéré comme une crise de santé mentale historique (Plante, 2020). Quoi qu'alarmant, le portrait actuel pourrait favoriser l'adoption de services qui s'inscrivent dans la prévention de différents enjeux de santé mentale comme ceux que proposent EmoScienS.

Manque de confiance : Le rapport de « Surmonter les risques, instaurer la confiance » de la série « Impératif de l'IA au Canada » de Deloitte (2019) dépeint l'enjeu de confiance comme un obstacle de taille à l'adoption des technologies d'intelligence artificielle. Le rapport note le manque d'éducation et de compréhension de l'univers de l'IA, de ses capacités et de ses utilisations actuelles et potentielles comme un grand frein à la confiance des consommateurs puisque l'idée qu'ils se font de l'IA demeure issue de la science-fiction. Cette situation peut jouer en la défaveur d'une technologie aussi intrusive et pouvant facilement jouer dans l'imaginaire de la population que celle d'EmoScienS.

Télétravail : Les nouvelles mesures de santé publique obligent les organisations à revoir leurs espaces de travail et forcent la majorité d'entre elles, faute d'espace adapté à la distanciation sociale, à adopter le télétravail (Langlais, 2020). Ce nouvel arrangement, largement plus répandu

qu'il ne l'était, brouille la limite entre la sphère professionnelle et personnelle des employés. Effectivement, une grande proportion d'entre eux se retrouvent à travailler à la maison, un espace privé, parfois entourés des membres de leur famille. Ce contexte offre une certaine flexibilité en ce qui a trait à la gestion du temps, faisant en sorte que les journées de travail sont parfois entrecoupées de moments privés rendant difficile de tracer la ligne les sphères personnelle et professionnelle (Leduc, Houlihan, Cameron, McConnell, Sadovnick et Erickson, 2020). Ces chevauchements potentiels pourraient compromettre l'acceptation sociale d'une technologie comme celle que propose EmoScienS. Effectivement, le télétravail impliquerait que cette technologie fonctionne et capte les émotions des individus alors qu'ils sont à leur résidence privée, à s'adonner à des activités qui ne sont pas exclusivement performées dans le cadre de leurs fonctions personnelles, pouvant générer un malaise.

3.1.4 Perspective technologique

Le port du masque : Le port obligatoire du masque pour répondre aux mesures de santé publiques qu'oblige la pandémie actuelle soulève des questions quant à la performance des systèmes de reconnaissance faciale dans ces conditions (Simonite, 2020). Vu la dépendance des systèmes de reconnaissance des émotions faciales à l'accès visuel des expressions faciales, il est à prévoir que le port du masque quotidien puisse avoir un impact sur la performance de ces technologies et que cette nouvelle réalité appelle à leur adaptation.

Reconnaissance faciale : Les technologies de reconnaissance faciale sont de plus en plus utilisées, mais sèment la controverse en raison de leur déploiement à des fins de surveillance ainsi que des risques qu'elles portent à la vie privée des individus (Castets-Renard, Guiraud et Avril-Gagnon, 2020). Les technologies de reconnaissance des émotions à travers les expressions faciales sont loin d'être faciles à différencier des technologies reconnaissance faciales pour le grand public, surtout que, de façon réaliste, celles-ci pourraient être combinées. Le caractère intrusif de la technologie que propose EmoScienS est susceptible de soulever des inquiétudes similaires qui pourraient compromettre son acceptabilité.

Technologies améliorant la confidentialité : Le rapport de Gartner « Top Strategic Technology Trends for 2021 » (2020) cite les TAC comme une arme indispensable pour continuer de prospérer de façon légale et responsable. Effectivement, quoiqu'elles ne soient pas nouvelles, ces technologies connaissent des avancées considérables qui permettront aux organisations de tirer profit de la valeur des données d'une façon sécuritaire et responsable qui répond aux nouvelles obligations légales que les régulations comme le RGPD posent. Ces technologies reçoivent beaucoup d'attention en raison des récentes découvertes relatives à la compromission de l'anonymat. Les organisations qui traitent des informations personnelles sensibles devront se munir de mesures de sécurité doublement robustes. Le rapport « *Protecting privacy in practice* » du *Royal Society* (2019) traite de techniques particulièrement efficaces à la protection des données sensibles, comme le chiffrement homomorphe, et adresse leurs capacités actuelles, limitations ainsi que leurs applications possibles. Il est à prévoir que ces techniques, toutes à différents stades de maturité, atteindront le stade de produit dans un futur proche et qu'il sera nécessaire pour les entreprises comme EmoScienS de prévoir les ressources et l'expertise nécessaires pour s'en munir.

Technologies éthiques : L'industrie des technologies devient hautement dépendante de la confiance que lui confèrent les utilisateurs. Cette confiance est dorénavant un passage obligé vers l'acceptation et l'adoption des nouvelles technologies qui, à elles seules, ne sont plus suffisantes pour assurer la compétitivité et la prospérité des organisations à l'ère du numérique. Les consommateurs sont soucieux de leur vie privée ainsi que de la sécurité de leurs données et sont de plus en plus exigeants à l'égard des pratiques organisationnelles. Ce mouvement appelle les organisations à changer leurs stratégies qui aujourd'hui se doivent d'être tournées vers l'humain, la collaboration et le bien-être de l'humanité. Le rapport d'Accenture « *Technology Vision 2020: We the Post-Digital People* » (2020) propose des tendances technologiques dans lesquelles les questions éthiques sont imbriquées alors que Deloitte en traite comme un mouvement à part entière (Bannister et Golden, 2020). Les rapports le prouvent, l'éthique n'est plus une question. L'éthique est le vecteur de différenciation sur lequel les organisations devront jouer pour espérer prospérer.

3.1.5 Perspective environnementale

Empreinte carbone de l'IA : Le sujet de l'empreinte carbone de l'IA commence à faire surface. Quoique très peu de chiffres existent sur le sujet, ceux qui circulent sont assez troublants. L'article « *Environmental sustainability and AI* » (Gow, 2020) suggère que même si l'empreinte carbone de toutes les technologies d'intelligence artificielle est différente, la notion de responsabilité environnementale très peu présente dans l'industrie de l'IA risque d'incomber toutes organisations du secteur, et ce, très prochainement. La situation est préoccupante dans la mesure où très peu est connu sur l'impact environnemental d'une industrie qui se développe à la vitesse grand V. Les chances sont que l'on se rende compte de ses impacts dévastateurs beaucoup trop tard, ce qui pourrait grandement affecter la réputation des organisations qui n'auront pas su y voir de façon proactive et dont les comportements à l'égard de l'environnement ne s'alignent pas avec les valeurs des consommateurs.

3.1.6 Perspective légale

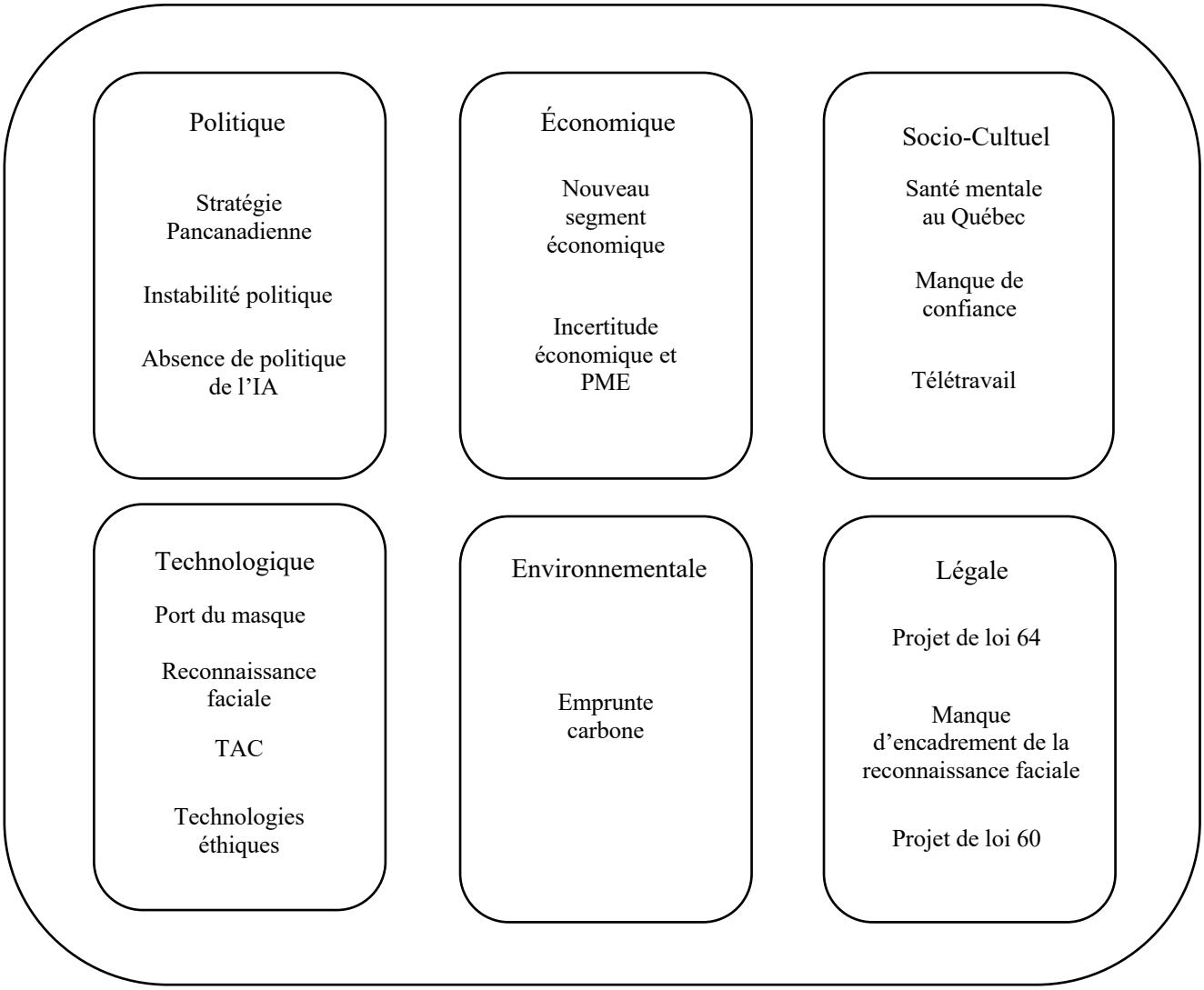
Modernisation des lois encadrant la protection des données personnelles: Les gouvernements québécois et canadien entreprennent la réforme des cadres législatifs encadrant la protection des renseignements personnels. Déposé devant l'Assemblée Nationale du Québec le 12 juin 2020, le projet de loi 64 du gouvernement québécois s'applique aux organismes publics et entreprises privées (Jolin-Barrette, 2020). Le gouvernement canadien, pour sa part, vient tout juste de déposer son projet de loi issu des consultations qui ont mené à la rédaction de la Charte canadienne du numérique et vise principalement les entreprises privées (Bordeleau, 2020). Ces deux projets visent notamment à mettre à jour certaines dispositions qui ne couvraient plus de façon convenable la question des données personnelles avec l'avancement des technologies et la modernisation des dispositions légales étrangères et prévoient des sanctions sévères pour les entreprises en faute. Ces projets de loi vont assujettir les organisations à des obligations plus grandes à l'égard de leur manipulation des données personnelles et fournir des droits aux utilisateurs qui s'apparentent à ceux prévus par le RGPD. La refonte arrive au bon moment, alors que l'UE, dotée de dispositions plus strictes depuis 2018, devra évaluer le caractère adéquat des protections offertes au Canada et au Québec pour permettre le transfert des données à caractère personnel de l'UE vers ces

territoires. Le projet de loi 64 devrait permettre au Québec et au Canada de se munir d'évaluations favorables permettant de faciliter les possibilités commerciales des entreprises d'ici avec le territoire de l'UE (Morgan, Joizil, Trottier, Bherer, Yifan Chen, 2020).

Encadrement insuffisant des technologies de reconnaissance faciale : L'Observatoire international sur les impacts sociétaux de l'IA et du numérique a publié un rapport sur le cadre juridique applicable à l'utilisation de la reconnaissance faciale (Castets-Renard, Guiraud et Avril-Gagnon, 2020). Les auteurs citent le projet de loi 64 comme un pas encourageant dans la bonne direction, mais soulignent que puisque les finalités de ce projet visent à renforcer la protection des données personnelles des consommateurs, il ne couvre pas l'ensemble des dangers inhérents aux technologies de reconnaissance faciale. Vu les nombreuses inquiétudes soulevées quant à l'utilisation de plus en plus répandue de ces systèmes, ce que la Commission de l'accès à l'information nomme dans son nouveau guide d'accompagnement à la biométrie (2020), il est à prévoir que des initiatives légales soient entreprises pour combler ce manque. Bien que la technologie d'EmoScienS soit différente du point de vue technologique, elle est encore plus intrusive par son traitement de données sensibles comme les émotions. À cet égard, il est à prévoir qu'une nouvelle loi encadrant l'utilisation de technologies biométriques puisse également viser les technologies d'informatique affective comme celles d'EmoScienS.

Projet de loi 60 - Modernisation de la loi sur la santé sécurité au travail : Un projet de loi visant à réformer le régime de santé et sécurité au travail a été présenté le 27 octobre dans le but d'adapter la LSST (loi sur la santé et sécurité au travail) et la LATMP (loi sur les accidents de travail et maladies professionnelles) aux réalités du marché du travail et d'améliorer les mesures de prévention des risques en milieu de travail (Ministère du Travail, de l'Emploi et de la Solidarité Sociale, 2020). Le projet de loi prévoit entre autres obliger les employeurs à mener des évaluations des risques psychosociaux dans leur programme de prévention, ce qui permettrait d'adresser l'enjeu de santé mentale au Québec selon le ministre responsable (Lévesque, 2020). Ce projet de loi est un pas intéressant dans la voie de la reconnaissance des enjeux de santé mentale et l'importance accordée à la prévention peut jouer en faveur d'EmoScienS qui propose une technologie tout à fait en accord avec ces objectifs.

Tableau 1 : Éléments de l'environnement externe d'EmoScienS



3.2 Conclusions de l'analyse PESTEL

De façon générale, cette analyse dépeint un portrait plutôt favorable à l'adoption d'une technologie comme celle que propose EmoScienS. Plusieurs remaniements légaux devant prendre effet dans un avenir très proche exerceront certainement de nouvelles contraintes sur les organisations, cependant, celles-ci ne sont qu'alignées avec le mouvement éthique dans lequel une entreprise comme EmoScienS s'inscrit. Plusieurs embûches engendrées par la pandémie actuelle forceront les entreprises à s'adapter et faire preuve de résilience devant cette nouvelle réalité, mais la

tendance éthique et le domaine de la santé psychologique et du bien-être auxquels EmoScienS prend part ne semblent pas perdre en puissance, bien au contraire. Effectivement, la santé mentale, la gestion des données personnelles et l'éthique des technologies demeurent des sujets d'actualité et d'inquiétudes, ce qui devrait permettre aux entreprises qui se positionnent dans ces créneaux de se démarquer. Malgré cela, la startup devra vraisemblablement faire preuve de doigté et de délicatesse dans son exercice de positionnement stratégique, vu l'absence de cadre légal régissant la création et l'utilisation des technologies d'intelligence artificielle ainsi que le caractère intrusif de la technologie qu'elle propose qui, dans l'imaginaire collectif, frôle la science-fiction.

L'analyse de l'environnement précédemment réalisée nous a permis de cerner les mouvements que l'environnement d'EmoScienS subit actuellement et sur lesquels elle n'a aucun contrôle. La section qui suit présentera un *benchmark* des pratiques éthiques d'organisations sélectionnées pour compléter le portrait de l'écosystème de la startup. Plus précisément, cette analyse en profondeur nous permettra d'identifier les éléments sur lesquels EmoScienS, en tant qu'acteur qui aspire à mener le bal du mouvement éthique, peut et doit agir pour se démarquer.

3.3 Analyse comparative des organisations de l'industrie

Selon Breidbach et Maglio (2020), l'avantage compétitif des organisations de l'industrie est appelé à changer. Les auteurs entrevoient que les pratiques actuelles puissent en fait ternir la réputation des organisations alors que les utilisateurs se conscientisent de plus en plus avec le temps, donnant un avantage sans précédent à celles qui sont éthiques (Breidbach et Maglio, 2020). En effet, ce changement ne serait pas surprenant alors que l'innovation constante à laquelle l'industrie des technologies a habitué la population ne semble plus leur suffire (Daugherty, Carrel-Billiard et Biltz, 2020). Les utilisateurs demandent autre chose de la part des corporations. Ils demandent plus. Certes, les gouvernements bougent lentement et les régulations se font attendre, mais rien n'empêche l'industrie de prendre les devants et paver la voie (Deloitte, 2019b). Tout de même, seulement quelques acteurs semblent se positionner dans l'angle de l'éthique des données, et encore, l'éthique n'est qu'un mot. Comme nous le verrons plus bas, ce mot est parfois opaque et doré de fioritures qui, de façon habile, dissimulent dans certains cas des pratiques qui sont tout sauf éthiques.

Afin de se positionner stratégiquement dans un environnement effervescent, EmoScienS a besoin de savoir ce que ses concurrents font, mais également ce qu'ils ne font pas. EmoScienS doit pouvoir repérer les angles morts, les opportunités inexploitées ainsi que les besoins en attente d'être comblés. Le présent *benchmark* nous servira donc à éclairer le chemin d'un positionnement stratégique avantageux pour la startup, lui permettant de surpasser ses concurrents tout en répondant aux attentes d'utilisateurs qui demandent transparence et respect de la part d'une industrie qui en a démontré que très peu jusqu'à maintenant.

Ce que ce *benchmark* contient

Le petit échantillon d'organisations présenté ci-bas représente une reconstitution approximative de l'environnement concurrentiel d'EmoScienS, une *startup* qui se situe à l'intersection entre plusieurs domaines d'expertise et dont les compétiteurs arborent différents visages. Le *benchmark* offre donc une certaine diversité en termes de missions, de technologies et de pratiques. Plus spécifiquement, les entreprises ont été sélectionnées sur la base de la technologie et du créneau qu'elles exploitent. L'échantillon contient donc des entreprises qui offrent une technologie d'informatique affective, toute modalité et tout domaine d'application confondu, ainsi que d'autres qui se positionnent dans le créneau de la santé mentale et du bien-être, à l'échelle individuelle ou organisationnelle, ou qui offrent des services centrés sur l'engagement et le bien-être des employés comme levier de performance organisationnelle.

Les limites de ce *benchmark*

Ce *benchmark* contient également plusieurs compromis et est limité de différentes façons. Certaines organisations, quoique très intéressantes, ont dû être éliminées du processus par manque d'accessibilité aux informations nécessaires afin de réaliser l'exercice d'analyse et de comparaison des pratiques éthiques que requiert ce *benchmark*. Il n'est évidemment pas exhaustif dans la mesure où il ne relate pas absolument toutes les pratiques relatives à la gestion des données personnelles et il reflète certaines limites de la compréhension que nous avons du domaine juridique. Ce *benchmark* est également limité aux informations volontairement divulguées par les organisations sur leur site internet qui ne sont pas toujours le reflet fidèle de leurs pratiques

organisationnelles, mais que nous avons dû tenir pour acquises dans le but de réaliser le présent exercice, faute d'accès aux faits véritables.

Ce que nous examinerons à travers ce *benchmark*

La structure de ce *benchmark* est inspirée de la définition de l'éthique des données de Floridi et Taddeo (2016, traduction libre : 3) qui va comme suit :

> « L'éthique des données est la branche de l'éthique qui étudie et évalue les problèmes moraux liés aux données (y compris la génération, l'enregistrement, la conservation, le traitement, la diffusion, le partage et l'utilisation), aux algorithmes (y compris l'intelligence artificielle, les agents artificiels, l'apprentissage machine et les robots) et aux pratiques correspondantes (y compris l'innovation responsable, la programmation, le piratage et les codes professionnels), afin de formuler et de soutenir des solutions moralement bonnes (par exemple, les bonnes conduites ou les bonnes valeurs) ».

Le *benchmark* débute donc par une courte introduction des organisations retenues pour l'exercice pour ensuite enchaîner avec une analyse de leur niveau d'éthique en les comparant sur divers critères issus de la définition présentée plus haut. Ensemble, les deux composantes de cette analyse devraient nous aider à dépeindre un portrait global des pratiques courantes dans l'industrie, ainsi que permettre à EmoScienS de faire des choix d'avant-garde en termes de gestion des données personnelles qui la positionnent au-devant de son écosystème.

3.3.1 Présentation des organisations

Affectiva, Inc.
https://www.affectiva.com/
Pays : États-Unis

Affectiva, Inc. (ci-après, « Affectiva ») offre entre autres une solution d'analytique média qui exploite l'informatique affective pour aider ses clients à améliorer leur contenu et l'expérience qu'ils offrent à leurs utilisateurs. Affectiva utilise une technologie de reconnaissance des émotions à travers les expressions faciales qui combine des techniques de vision artificielle et

d'apprentissage profond qui mesure sept émotions et 20 expressions faciales grâce à des algorithmes entraînés sur une banque de données d'émotions faciales de plus de 50 000 vidéos et 9.5 millions de visages à travers 90 pays. Les données émotionnelles des utilisateurs, recueillies à l'aide de leur webcam avec leur consentement, sont affichées sur un tableau de bord muni de normes d'industrie prêtes à la comparaison et permettent aux organisations d'avoir un meilleur aperçu du vécu émotionnel des utilisateurs lorsqu'ils visionnent différents contenus. Ces « *insights* » permettent à ces derniers de concevoir leur contenu avec une meilleure compréhension de la façon dont il est reçu par leur audience et ainsi améliorer leur performance.

Moodmetric par Vigofere Oy
https://Moodmetric.com/
Pays : Finlande

Moodmetric aide les individus à suivre leur stress au quotidien à l'aide d'une bague qui mesure et suit l'activité électrodermale en continu. Le dispositif est connecté à une application qui affiche les fluctuations de l'activité en temps réel sous forme de graphiques. L'application permet également la tenue d'un journal des activités qui sont ensuite analysées de pair avec les fluctuations de stress pour identifier les événements qui contribuent à ces variations, permettant ainsi à l'individu de développer une meilleure conscience de soi et d'ajuster ses habitudes de vie en conséquence. La solution est également offerte aux organisations qui voudraient adresser les enjeux de stress des groupes et des individus qui les composent afin de les accompagner dans la modification de leurs habitudes de vie.

Feel par Sentio Solutions Inc.
https://www.myfeel.co/
Pays : États-Unis et Grèce

Sentio Solutions Inc. (ci-après « Sentio Solutions ») offre le programme « Feel », un service de téléthérapie qui vise à supporter le vécu émotionnel des individus, ainsi qu'à aider ceux qui sont aux prises avec des enjeux de stress et d'anxiété. Le programme est constitué d'un bracelet connecté muni de cinq détecteurs qui mesurent et suivent en continu une série de signaux physiologiques ensuite traduits à l'aide d'algorithmes en quatre patrons émotionnels. Ces mesures

sont disponibles de façon instantanée sur une application qui offre aussi la possibilité d'entrer des informations manuellement dans un journal, ainsi qu'un service de support émotionnel par l'entremise d'interventions appropriées. L'application contient des programmes éducatifs visant à outiller les utilisateurs sur les habitudes positives de gestion d'émotions et le programme offre une séance de 15 minutes, à distance, avec un thérapeute. Le service est offert sur une base individuelle, ou encore aux organisations dans un but de prévention et d'accroissement de la motivation et de la productivité des employés.

DeepAffects par SeerNet Technologies LLC.
https://deepaffects.com/
Pays : États-Unis

DeepAffects est une plateforme web pour les équipes de travail virtuelle qui exploite l'informatique affective pour analyser les émotions des individus et les dynamiques d'équipe à travers la voix et le langage écrit via une série de onze métriques disponibles sur la plateforme. La plateforme génère des « *insights* » quant à la charge émotionnelle, les possibilités de conflits et les problèmes d'engagement par exemple, pour aider les cadres et les équipes à évaluer les enjeux émotionnels, améliorer les dynamiques et la productivité.

Behavioral Signal Technologies, Inc.
https://behavioralsignals.com/
Pays: États-Unis

Behavioral Signal Technologies, Inc. (ci-après « Behavioral Signal ») offre deux solutions d'intelligence artificielle principalement conçues pour les centres d'appels : « *Voice Intelligence Analytics* » et « *AI-Mediated Conversations* ». La première solution analyse les conversations agents-clients à l'aide de plusieurs mesures comme la politesse, l'agitation, le niveau d'empathie, la réaction du client et certaines caractéristiques dans la voix pour calculer un score de la qualité de la conversation et mesurer la performance de l'agent. Cette solution permet de repérer le moment exact où une conversation dérape par exemple, et offre un outil de transcription automatique qui identifie les composantes émotionnelles et comportementales de la conversation pour pouvoir mieux analyser la performance des employés, les supporter dans le développement

de leurs « *soft skills* » et mieux accompagner les consommateurs lors des appels. La deuxième est une solution automatisée qui utilise l'informatique affective et les données vocales pour jumeler le client avec l'agent le plus disposé à traiter l'appel. En optimisant le niveau d'affinité entre le client et l'agent, l'organisation peut améliorer la performance de ses employés, leur satisfaction et celle de la clientèle, ainsi que réduire les coûts reliés aux appels non résolus et non productifs.

Dialogue Technologies Inc.
https://www.dialogue.co/en/
Pays : Canada, Québec

Dialogue Technologies Inc. (ci-après « Dialogue ») offre un service de télémédecine aux organisations pour les aider développer une culture axée sur la santé et le bien-être au travail ainsi qu'à adresser les enjeux de santé physique et mentale des employés pour augmenter leur engagement et leur productivité. En plus d'autres services, Dialogue offre un programme d'assistance employé qu'elle opère sur une plateforme de santé intégrée offrant des services de consultation et d'orientation dans une panoplie de sphères, comme le stress et le bien-être, le conseil juridique et financier, la famille et les relations ainsi que le travail et la carrière. Elle permet aux employés d'avoir accès à une foule de services en un seul endroit, avec accès à une consultation ou rencontre d'orientation dans un délai de 24 heures.

Modern Health par Modern Life Inc.
https://www.joinmodernhealth.com/
Pays : États-Unis

Modern Health est une plateforme intégrée de soins de santé mentale offerte aux employés d'organisations à travers le monde. Elle offre un service de consultation psychologique basée sur une approche cognitive comportementale ainsi que des sessions de coaching avec des professionnels certifiés. La plateforme offre également des ressources digitales, comme des cours ciblés et des techniques de méditation pleine conscience. L'ensemble de ces services facilite l'accès au support psychologique dont les employés ont besoin, lorsqu'ils en ont besoin. Ceux-ci sont déterminés sur une base individuelle à l'aide de questionnaires autoadministrés et validés

scientifiquement qui permettent d'établir un plan de match personnalisé combinant les différentes ressources sur la plateforme.

LifeWorks Canada Ltd
https://www.lifeworks.com/ca/fr/
Pays : Canada

LifeWorks Canada Ltd (ci-après « LifeWorks ») est une plateforme de mieux-être global des employés qui intègre une multitude de fonctionnalités dédiées à l'expérience humaine en organisation dans le but de renouveler les programmes d'aide aux employés traditionnels et d'en créer qui répondent aux besoins des employés d'aujourd'hui. En ce qui a trait à la santé psychologique, la plateforme offre un service de support professionnel et personnel en ligne et en tout temps, ainsi que du contenu digital personnalisé et varié orienté vers le mieux-être. La plateforme comporte également un axe « mieux-être physique » qui permet de supporter les employés dans leurs défis personnels et de les motiver à adopter des habitudes de vie saine à l'aide d'évaluations de santé, de recommandations personnalisées, de ressources appropriées ainsi que du contenu interactif et éducatif traitant de sujets diverses passant de la gestion du stress à la gestion du poids. La plateforme offre également un fil de reconnaissance qui permet aux employés de souligner les bons coups, de partager les bonnes nouvelles et la progression individuelle pour créer une culture de reconnaissance et de support.

Peakon par Peakon ApS
https://peakon.com/us/
Pays : Danemark

Peakon ApS (ci-après « Peakon ») offre une plateforme de « succès employé » qui permet de recueillir les sentiments, impressions et opinions des employés à l'aide de sondages personnalisés. Ces sondages permettent aux organisations d'être à l'écoute des employés, de prendre des actions concrètes pour favoriser leur engagement et le mettre à profit de la performance des organisations. La plateforme de Peakon offre une multitude de fonctionnalités basées sur les résultats de sondages qui sont analysés en temps réel et qui, grâce à des techniques de *natural language processing*, permettent d'identifier les facteurs clés sur lesquels agir. À travers ses différents programmes

d'adhésion, Peakon offre l'opportunité pour l'organisation de se comparer à l'industrie, mais aussi à l'interne avec son outil *True Benchmark* qui utilise l'apprentissage machine pour dériver des scores d'engagements qui tiennent compte du profil unique de chaque employé. Elle offre également la possibilité de personnaliser les sondages futurs sur la base des résultats actuels pour permettre d'orienter la conversation vers les sujets les plus susceptibles d'offrir une compréhension toujours plus pointue des enjeux organisationnels et offre du support à l'action avec des suggestions adaptées aux résultats de sondages.

Bloom par Meemo Media, Inc.
https://www.enjoybloom.com/
Pays : États-Unis

Bloom est une application mobile qui fournit un support psychologique quotidien à ses utilisateurs basé sur les principes de la thérapie cognitive comportementale pour les aider à gérer leur stress et leur anxiété ainsi qu'améliorer leur santé psychologique et leur bien-être général. L'application combine plusieurs modalités d'interventions, comme les classes interactives en ligne dont le contenu est conçu à l'aide des derniers résultats de recherche en matière de santé mentale, de thérapeutes et psychologues, la tenue d'un journal porté sur les pensées et les émotions et guidé par des principes ancrés dans l'approche cognitive comportementale ainsi que des exercices de pleine conscience pour améliorer le sentiment de bien-être de ses utilisateurs.

My Possible Self par My Possible Self Limited
https://www.mypossibleself.com/
Pays: United Kingdom

My Possible Self Limited (ci-après « My Possible Self ») est une application mobile qui vise à aider ses utilisateurs à adresser leurs enjeux de santé mentale personnels à travers une meilleure connaissance de soi et le développement de la capacité d'autogestion, pour leur permettre de mieux naviguer les situations difficiles du quotidien. Ancrée dans un mélange principes relevant d'une approche cognitive-comportementale, de thérapie interpersonnelle, de résolution de problème et de psychologie positive, l'application offre plusieurs fonctionnalités, donc dix modules ciblant des enjeux spécifiques pour aider à développer de nouvelles habiletés, un « *mood tracker* » qui permet

l'entrée d'informations comme des photos, des lieux, des activités qui permettent de développer une meilleure conscience des éléments qui influencent le vécu émotionnel, ainsi que le « *mood history* » qui permet un regard rétrospectif sur les variations et la progression des humeurs dans le temps. L'application My Possible Self est également offerte aux entreprises qui veulent promouvoir une culture de santé bien-être qui favorise la satisfaction, l'engagement et la productivité de leurs employés grâce au développement d'habiletés qui favorisent une meilleure gestion de leurs enjeux de santé mentale et un sentiment de support psychologique au travail.

Rise par Rise, Inc.
https://www.risescience.com/
Pays : États-Unis

Rise, Inc. (ci-après « Rise ») est une application qui calcule à elle seule la biologie du sommeil des individus, sans l'aide de dispositif physique autre que le téléphone. Elle personnalise l'expérience de ceux-ci autour de ce profil et de leurs défis pour améliorer leur dette de sommeil, l'indicateur par excellence de la performance quotidienne selon l'entreprise. L'application créer des horaires précis pour aider les individus à prendre conscience de la façon dont leur biologie influence leur journée, ainsi qu'à reconnaître les moments les plus ou moins propices à la productivité. L'application offre également des conseils pour améliorer la dette de sommeil et favoriser des habitudes de sommeil saines et sa version payante donne l'accès exclusif à un coach de sommeil. Rise offre également ses services aux entreprises. Elle permet d'optimiser la performance des équipes grâce à l'amélioration du sommeil des employés. L'application offre l'opportunité de déterminer les moments les plus susceptibles d'être productifs pour les individus et les équipes et de retirer le maximum de ceux-ci pour augmenter la performance et les revenus.

3.3.2 Comparaison des organisations

La section qui suit comparera les douze organisations recensées dans la section précédente sur un ensemble de critères inspirés de la définition de l'éthique de données de Floridi et Taddeo (2016) citée plus haut. Nous débuterons en abordant la transparence et l'accessibilité de l'information, catégorie qui se décline en quatre sous-composantes, soit le niveau de transparence relatif à la technologie, l'accessibilité, la clarté et l'exhaustivité de l'information disponible. Nous traiterons

ensuite, sous la section des pratiques relatives à la gestion des données personnelles, de la collecte, de l'utilisation, du partage et de la vente, de la rétention, de la sécurité et l'entreposage des données, ainsi que de l'utilisation des témoins. Nous traiterons ensuite des droits que ces organisations fournissent à leurs utilisateurs, pour finalement terminer avec une courte section sur les initiatives organisationnelles.

Transparence et accessibilité de l'information

Niveau de transparence relatif à la technologie

Considérant qu'il est naturel pour celles-ci de conserver un certain niveau de confidentialité vu la valeur concurrentielle de leur technologie, les organisations qui font l'utilisation de technologies d'informatique affective ou d'intelligence artificielle n'offrent pas toutes le même niveau de transparence à l'égard de leur technologie.

Parmi les plus transparentes se trouvent Moodmetric et Affectiva. En plus de dédier une page à l'explication détaillée de leur technologie, les deux entreprises divulguent le niveau d'exactitude de leurs algorithmes et offrent l'accès rapide à des études reliées sur leur site internet. Affectiva mentionne également des informations relatives à la banque de données qu'elle utilise pour entraîner son algorithme et la façon dont ces données sont collectées.

Les autres organisations traitent de leur technologie de façon plus ou moins vague. Par exemple, SS se contente de nommer les biomarqueurs que son algorithme utilise en mentionnant que ceux-ci sont ceux qui sont rapportés par la recherche comme étant les plus exactes dans la prédiction des émotions. Elle offre une petite section qui explique très brièvement les fondements de sa technologie sans offrir de détails tangibles.

Pour leur part, Behavioral Signal et Rise expliquent les fondements de leurs technologies, mais de façons bien différentes. Behavioral Signal offre une section à plusieurs onglets entièrement dédiée à l'explication de l'informatique affective, de la reconnaissance des émotions, du champ d'étude qu'elle a développé, le *Behavioral Signal Processing*, ainsi qu'un *White Paper* qui entre dans les détails de cette technologie. De son côté, Rise offre des explications qui se retrouvent dans son

blog. Il n'est pas évident que le blog soit dédié à l'explication de sa technologie et il faut aller lire les différents articles pour comprendre qu'ils ont été écrits pour aider le lecteur à comprendre de quelle façon la technologie de Rise peut l'aider. Les explications sont présentes, mais loin d'être mises en évidence.

Accessibilité de l'information

En termes d'accessibilité, Peakon se démarque largement par la facilité de navigation sur son site internet. Effectivement, sa politique de vie privée contient différentes sections portant des noms clairs ainsi que des onglets qui permettent de passer d'une section à l'autre en un simple clic. Sa politique de vie privée principale offre également un lien qui mène à sa politique de vie privée marketing. Elle traite séparément de son utilisation des témoins (*cookies*) dans une politique à part et offre à même son internet site une page permettant de désactiver les témoins, évitant aux utilisateurs d'aller s'égarer dans les paramètres de leur navigateur web. Sur le site de Peakon, tout est facilement accessible et toute l'information nécessaire s'y trouve.

L'information n'est pas aussi facilement accessible les sites internet de DeepAffects et de Rise, par exemple. La politique de vie privée de DeepAffects et les conditions d'utilisation de Rise sont impossibles à trouver sur le site internet des deux entreprises. Ils ne contiennent aucun lien vers les pages en question et il faut les chercher dans un moteur de recherche internet externe pour finalement être redirigé sur les pages appropriées qui, ironiquement, se trouvent sur leurs sites respectifs. Aussi, la politique de vie privée que Rise offre sur son site est très courte et ne se résume qu'à quelques points saillants, alors que celle qu'elle offre sur la page de son application sur le Apple Store est plus extensive. Les deux politiques ne sont pas identiques et, sans se contredire, elles sont à tout le moins incomplètes l'une sans l'autre, ce qui peut semer la confusion.

Clarté de l'information

En ce qui a trait à la clarté des propos et la disponibilité d'une information compréhensible pour l'utilisateur, Peakon est toujours en tête de liste et suivie de près par LifeWorks. Effectivement, les efforts de Peakon sont considérables et se traduisent en une politique de vie privée et des conditions d'utilisations qui, grâce à un vocabulaire accessible et de multiples exemples concrets, sont faciles à lire et à comprendre. L'organisation offre également une page et une foire aux

questions dédiées au RGPD, en plus de sa politique de vie privée. Ces deux pages résument et vulgarisent l'information pertinente pour l'utilisateur, sans jamais insinuer qu'elles sont suffisantes à elles seules. Elles contiennent plusieurs liens vers la politique de vie privée de Peakon pour que l'utilisateur puisse compléter l'information et accéder à tous les détails.

Pour sa part LifeWorks offre une politique de vie privée longue, mais très claire et compréhensible. Notamment, elle contient un tableau qui répertorie toutes les catégories d'informations personnelles que l'organisation collecte, les données exactes que cela comprend et à quelles fins elles seront utilisées. En rendant l'information visuellement beaucoup plus claire et compréhensible pour le lecteur qui, autrement, peut facilement se perdre dans le texte continu et les énumérations sans fin typiques des autres politiques de vie privée, LifeWorks se démarque de la majorité des politiques de vie privée consultées dans le cadre de ce *benchmark*. Ses conditions d'utilisation sont considérablement plus courtes et concises que celles de l'ensemble des autres organisations, notamment en raison du fait qu'elle ne contient pas de clauses de non-responsabilité, de limitation de responsabilité, d'indemnité ou encore de sections sur l'arbitrage et les disputes par exemple.

DeepAffects fournit un effort de vulgarisation en marge de ses conditions d'utilisation qui, à la base, sont assez claires comparées à celles des autres organisations. Ses conditions d'utilisation sont rédigées dans un langage plus « amical » qui contraste fortement avec la lourdeur et l'agressivité qui se dégage de la majorité des autres conditions d'utilisation consultées.

Finalement, Affectiva offre une politique de vie privée rédigée dans des termes relativement clairs, mais dont la structure est désordonnée. Sa politique répète de nombreuses sections, sans aucune explication. Il est impossible de savoir pour quelle raison ces sections se répètent ou si elles sont supposées s'appliquer à d'autres contextes, ce qui porte à confusion.

Exhaustivité de l'information disponible

Toute l'information pertinente n'est pas nécessairement disponible sur le site des entreprises, surtout en ce qui concerne la façon dont ces dernières traitent les informations personnelles des utilisateurs dans leur double rôle de responsables du traitement et de sous-traitants.

Effectivement, la plupart des organisations qui font partie de ce *benchmark* offrent des services organisationnels qui sont propulsés par les données utilisateurs, donc les données des employés. Dans cette relation, les organisations qui font partie de ce *benchmark* agissent en tant que sous-traitants et traitent les informations pour l'organisation cliente. Les conditions de cette relation, notamment en ce qui a trait au traitement des données et les responsabilités respectives des deux parties relatives à la protection des données utilisateurs, sont déclarées dans un contrat de traitement des données qui n'est que très rarement divulgué sur le site des organisations. Celles-ci jouent également le rôle de responsables en ce qui a trait aux données personnelles qu'elles traitent à travers leur site internet. Certaines organisations mentionnent à quels moments elles agissent en tant que responsables et sous-traitants, mais il n'est pas toujours clair ce que leur politique de vie privée couvre.

À cet effet, un exemple flagrant est celui de DeepAffects. Comme il est naturellement le cas, ses conditions d'utilisation et sa politique de vie privée se chevauchent et se complètent. Cependant, à aucun moment l'organisation ne fait une mention claire de la portée de chacun de ses documents légaux à travers ses différentes capacités, qu'elle ne précise pas non plus. Il n'est donc pas évident de déterminer l'applicabilité des différentes dispositions contenues dans ses documents, surtout qu'elle fait plusieurs va-et-vient entre les documents qui, à eux seuls, ne couvrent même pas l'ensemble des informations nécessaires. Effectivement, aucun des documents ne spécifie les droits fournis aux utilisateurs ou encore les pratiques de rétention. Le seul endroit où ces informations pourraient être couvertes est le *service-level agreement* (SLA), un équivalent du contrat de traitement des données, qu'elle mentionne à plusieurs reprises dans ses conditions d'utilisation, sans jamais en divulguer le contenu.

Pour sa part, Behavioral Signal stipule clairement que sa politique de vie privée ne s'applique pas aux données qui sont traitées dans ses capacités de sous-traitant qui, elles, sont couvertes exclusivement par le contrat de traitement des données entre Behavioral Signal et les organisations clientes. Les protections offertes dans la politique sont donc limitées aux informations personnelles collectées à travers son site. Affectiva adopte une approche similaire et mentionne que dans les contrats de traitement qu'elle a avec ses clients peuvent comporter des clauses concernant la

rétention et l'utilisation des données qui diffèrent de sa politique de vie privée générale et qui ont préséance sur celle-ci.

De leurs côtés, Peakon, LifeWorks et Rise adoptent des positions plus transparentes et directes. Effectivement, Peakon offre deux politiques de vie privée qui couvrent les données qu'elle collecte dans ses capacités de responsable et de sous-traitant. Elle offre également une copie de son contrat de traitement des données en annexe de ses conditions d'utilisation. De leur côté, Rise et LifeWorks offrent des politiques de vie privée qui s'appliquent à l'ensemble de leurs services. LifeWorks offre également une politique de vie privée qui vise les informations récoltées à travers les appareils électroniques ainsi qu'une politique exclusive à l'intention des résidents de l'UE et de l'Angleterre.

Choix des pratiques

Au niveau de la collecte

Au niveau de la collecte des données, très peu d'organisations s'engagent à ne collecter que le minimum d'informations nécessaires pour fournir leurs services. Il n'y a que Moodmetric et Rise qui sont très épurées dans leur approche et qui énumèrent les quelques données dont elles se contentent. Les autres organisations collectent beaucoup plus de données et couvrent une série de catégories de données autres que celles nécessaires pour ou résultant de la prestation de leurs services. Certaines recueillent même des informations personnelles par l'entremise de tiers et leurs façons de les traiter peuvent différer.

Par exemple, dans sa poitique de vie privée Sentio Solutions (2020) stipule que « si [elle] combine ou associe ces informations provenant de d'autres sources avec des données personnelles recueillies par le biais de [ses] services [elle les traitera] comme des données personnelles conformément [à sa politique de vie privée] ». Ce passage laisse entendre qu'autrement, ces données personnelles ne possèdent pas le même niveau de protection que celles que Sentio Solutions collecte elle-même. De son côté, Behavioral Signal adopte une approche plus transparente et stipule clairement que « les données à propos des individus qui sont accessibles sur les plateformes de médias sociaux comme Facebook, LinkedIn, Twitter et Google, ou celles

acquises des fournisseurs de services » (2020) sont des données personnelles et donc, qu'elles sont automatiquement traitées de la sorte.

Affectiva est la seule organisation qui utilise exactement la même technologie de reconnaissance des émotions à travers les expressions faciales. Sa politique de vie privée stipule clairement que la collecte des enregistrements vidéo et audio, toujours collectés suite à l'obtention d'un consentement éclairé, peut également « inclure des métadonnées et des données de localisations » (Affectiva, Inc., 2020, traduction libre). Elle mentionne que les données d'expressions faciales et vocales ne sont jamais traitées de pair avec des données personnelles qui pourraient mener à l'identification des sujets, et que ces données ne seront « jamais associées à un individu sans [son] consentement » (Affectiva, Inc., 2020, traduction libre).

La majorité des organisations collectent des données « non personnelles ». Cette catégorie de données comprend des données personnelles qui sont collectées sans être liées à un identifiant, ou encore des données qui sont anonymisées et agrégées suite à leur collecte. Étant considérées « non personnelles », ces données ne sont pas traitées avec la même discrétion que les données personnelles. Cette distinction est importante et potentiellement hautement problématique pour des raisons exposées dans la revue de littérature plus haut que nous visiterons de nouveau dans la section ci-bas.

Au niveau de l'utilisation, du partage et de la vente

Les organisations varient considérablement en termes de l'utilisation qu'elles font des données personnelles. Certaines, comme Moodmetric, DeepAffects et Bloom, sont assez minimalistes et se restreignent à quelques utilisations, alors que Peakon, Sentio Solutions, et LifeWorks possèdent une liste d'utilités possibles assez impressionnantes. Aussi, toutes ne sont pas aussi transparentes et détaillées dans leurs descriptions. Par exemple, Rise et Modern Health traitent de l'utilisation des données personnelles de façon plutôt vague. Les deux organisations possèdent une section conjointe traitant des types de données collectées et de leurs utilités, au lieu de les traiter séparément comme la majorité des autres organisations. Cependant, ces sections dans les politiques des deux entreprises s'avèrent à ne mentionner que très rarement, voire jamais, la façon dont elles les utilisent les données personnelles. D'autres, comme Sentio Solutions, utilisent des

formulations pleines de sous-entendues comme : « Lorsque le droit applicable l'exige, nous ne traiterons les données personnelles sensibles qu'avec votre consentement » ou encore « en règle générale, vous pouvez refuser de recevoir toute communication promotionnelle […]. Lorsque la législation en vigueur l'exige, nous ne vous enverrons des courriers électroniques promotionnels qu'avec votre consentement » (Sentio Solutions Inc, 2020, traduction libre). Ces propos laissent entendre que SS utilise la loi à son avantage plus qu'elle ne l'utilise comme base solide sur laquelle bâtir des pratiques éthiques envers les données personnelles et les utilisateurs.

Peakon et Sentio Solutions, sont les deux seules organisations qui mentionnent explicitement l'utilisation des données personnelles, incluant les données sensibles pour Sentio Solutions, à des fins de recherche. D'autres organisations, comme Moodmetric, Dialogue, My Possible Self et LifeWorks font mention de ces utilisations, mais précisent qu'elles n'utilisent que les données anonymisées, dépersonnalisées et agrégées à ces fins. Affectiva évoque aussi l'utilisation des données personnelles pour « la recherche ou [des] expérimentations plus larges », mais note qu'elle donne la possibilité aux utilisateurs de « [faire le choix explicite] de permettre l'utilisation de leurs données vidéo à [ces fins] » (Affectiva, Inc., 2020, traduction libre). Malgré qu'elle mentionne qu'elle ne partage pas les données issues d'enregistrements vidéo et audio sans les avoir préalablement anonymisées avec des tiers, sa politique de vie privée ne mentionne pas clairement si cette condition s'applique au contexte de recherche qu'elle mentionne, ou encore si ces recherches sont conduites par elle ou par des tiers, ce qui peut avoir plusieurs implications.

Pour sa part, Modern Health est l'organisation qui offre le moins de transparence. Effectivement, alors que sa politique de vie privée possède une section supposée traiter de l'utilisation des données personnelles et qu'elle n'en fait mention à aucun moment, c'est à travers ses conditions d'utilisation considérablement longues et denses qu'elle en traite. On peut y lire notamment que :

> « La Société n'a pas le droit de sous-licencier ou de revendre les Données de l'Utilisateur, à l'exception du fait que vous acceptez que la Société puisse collecter, analyser et utiliser les données dérivées des Données de l'Utilisateur, qui peuvent inclure des données personnelles et/ou des informations collectées auprès d'un individu ou à son sujet, mais qui ne l'identifient pas personnellement, ainsi que des données vous concernant et concernant l'accès et l'utilisation du Service par d'autres Utilisateurs, dans le but d'exploiter, d'analyser, d'améliorer ou de commercialiser le Service et tous les services connexes. Si la

> société partage ou divulgue publiquement des informations (par exemple, dans des documents marketing ou dans le développement d'applications) qui sont dérivées des données de l'utilisateur, ces données seront agrégées ou rendues anonymes afin d'éviter raisonnablement l'identification d'un individu spécifique ou de l'utilisateur. À titre d'exemple et sans limitation […]. Vous acceptez en outre que la société ait le droit, pendant et après la durée des présentes conditions, d'utiliser, de stocker, de transmettre, de distribuer, de modifier, de copier, d'afficher, d'accorder des sous-licences et de créer des œuvres dérivées des données anonymes et agrégées. Voir la politique de confidentialité de Modern Health » (Modern Life Inc., 2019, traduction libre).

Cette clause révèle plusieurs de pratiques dont Modern Health ne traite que peu ou pas du tout dans sa politique de vie privée, ce qui rend la dernière phrase du passage particulièrement ironique. Par ailleurs, il est inhabituel et questionnable qu'elle ait choisi de traiter de ces informations dans ses conditions d'utilisation, alors qu'il est raisonnablement attendu par la plupart des lecteurs que ce genre d'information se retrouve dans une politique de vie privée, comme il est le cas pour l'ensemble des organisations explorées dans ce *benchmark*. Ce choix pourrait paraître comme un effort de dissimulation de données pertinentes et importantes, sans quoi l'utilisateur ne peut prendre une décision réellement éclairée.

La distinction entre les données personnelles et les données anonymisées, dépersonnalisées et agrégées n'est pas toujours évidente pour le lecteur et, alors que cette distinction a beaucoup d'implications, ce ne sont pas toutes les organisations qui les distinguent clairement. Effectivement, la majorité des pratiques mentionnées dans les politiques de vie privée des organisations de ce *benchmark* ne concernent que les données personnelles. Lorsque des organisations comme Behavioral Signal, et DeepAffects mentionnent qu'elles ne vendent pas les données personnelles, quoiqu'elles fassent partie des rares qui le disent de façon explicite, on ne peut raisonnablement conclure qu'elles ne vendent aucune donnée, puisque les données personnelles concernent exclusivement les données personnellement identifiables. Les chances sont donc qu'elles vendent des données, mais de façon agrégée, anonymisée et dépersonnalisée. Il est tentant de penser que cette pratique ne va pas à l'encontre de principes éthiques puisqu'elle préserve supposément l'anonymat des personnes, mais comme souligné dans la revue de littérature plus haut, il a été prouvé que ces données peuvent être identifiées de nouveau et qu'elles révèlent beaucoup d'informations utiles au sujet des groupes permettant aux organisations de les cibler.

Les organisations partagent les données anonymisées, dépersonnalisées et agrégées à une multitude d'acteurs, que ce soit les membres d'un même groupe commercial, des filiales, des tiers de confiance ou encore d'autres organisations qui en feront usage à des fins statistiques. Ces acteurs qui sont tenus de respecter la politique de vie privée de l'organisation qui partage les données et de ne pas en faire usage de façon personnelle n'ont pas les mêmes obligations envers les données « non personnelles ». Effectivement, la quasi-totalité des clauses que contiennent les politiques de vie privée d'entreprises concerne exclusivement les données personnelles. Ces données potentiellement réidentifiables et très révélatrices d'informations précieuses pour les groupes se retrouvent à être partagées en continu et utilisées à des fins secondaires potentiellement néfastes. Cette pratique est donc loin d'être innocente et sans risque. Alors que pratiquement toutes les organisations de ce *benchmark* l'adoptent, seulement Dialogue et My Possible Self font la distinction claire entre les données personnelles et les données anonymisées, dépersonnalisées et agrégées dans la section qui spécifie les informations qu'elles collectent de leur politique de vie privée respective. Pour sa part, Peakon mentionne que le droit à l'effacement ne s'applique pas aux données anonymisées, dépersonnalisées et agrégées, mais de façon très isolée. Effectivement, le reste de sa politique est ponctué de mentions sporadiques des droits qu'elle se réserve face à ces données sans jamais en spécifier la distinction.

Malgré les limites de la portée des propos d'une organisation qui stipule qu'elle ne partage pas les données personnelles pour les raisons exposées plus haut, il demeure que toutes les organisations n'adoptent pas la pratique avec la même retenue et la même transparence. Effectivement, certaines comme Rise et Moodmetric mentionnent clairement qu'elles ne partageront jamais les données personnelles, ce à quoi Moodmetric pose une exception, soit lorsque la demande vient de l'utilisateur. Dans cette éventualité, Moodmetric rédige un contrat séparé et limitant à l'intention d'un tiers ciblé, et lui fournit les informations personnelles après avoir obtenu le consentement explicite de l'utilisateur en question.

Les autres organisations s'adonnent ouvertement au partage des données personnelles, quoique ce partage soit habituellement restreint à des situations spécifiques et seulement avec des tiers ciblés qui sont tenus de ne pas utiliser les informations à des fins personnelles et de respecter la politique de vie privée de l'organisation qui les partage. Certaines offrent moins de détails que d'autres

quant aux circonstances de ce partage ou à l'identité des tiers, mais encore une fois Peakon se démarque en nommant explicitement les destinataires de ces données personnelles.

Toutes les organisations ne sont pas explicites quant au partage des données anonymisées, dépersonnalisées et agrégées. La majorité, incluant Behavioral Signal, LifeWorks, Bloom, Modern Health, Dialogue et My Possible Self mentionnent de façon très claire la possibilité qu'ils partagent ces informations à des tiers. Sentio Solution (2020, traduction libre), pour sa part, mentionne l'utilisation de ces données « à d'autres fins » que celles précédemment mentionnées, alors que Moodmetric (2020, traduction libre) évoque qu'elle peut les utiliser pour « des fins commerciales », ce qui laisse place à plusieurs interprétations, dont certaines semblent aller à l'encontre de l'impression générale que laisse Moodmetric à travers son site et sa politique de vie privée.

Finalement, Affectiva mentionne, encore une fois de façon plus ou moins claire, qu'elle « ne vend ou ne loue pas les informations personnelles à d'autres à moins qu'une permission ait été donnée à l'avance, [qu'elle] ne vend ou ne loue pas les informations personnelles à des tiers pour des raisons autres que celles mentionnées [dans sa politique de vie privée] et [qu'elle] ne vend pas les informations personnelles [au sens] défini par le CCPA » (Affectiva, Inc., 2020, traduction libre). Il est à noter que quoique le *California Consumer Privacy Act* (CCPA) « possède de hauts standards pour considérer les informations dépersonnalisées et agrégées, la régulation ne restreint pas l'organisation dans la vente de données personnelles dépersonnalisées ou agrégées » (Jehl, Friel, Bakerhostetler LLP et Practical Law Data Privacy Advisor, 2018, traduction libre). La délicatesse avec laquelle Affectiva aborde le sujet de la vente de données personnelles, bien illustrée par le passage précédent, laisse entendre que c'est possiblement ce qu'elle fait et porte à interprétation.

Au niveau de la rétention

La majorité des organisations offre un discours similaire quant à la rétention des données. Il est relativement rare de voir une organisation qui, en plus de nommer les délais, les garde au minimum requis pour pouvoir assurer ses services. Rise est la seule d'entre toutes qui s'engage à ne conserver les données personnelles que pour une durée de 60 jours. D'autres organisations, comme My Possible Self et Peakon offrent des délais tangibles, mais sujets à changement et qui varient

grandement d'une situation à l'autre. Effectivement, My Possible Self mentionne que ces délais ne sont que des lignes directrices et Peakon offre trois scénarios de rétention et donne préséance à celui qui survient le premier. Cependant, Peakon fait également la mention qu'après ce délai l'information est soit anonymisée ou supprimée et se réserve le droit de conserver les données agrégées et anonymisées indéfiniment. Cette mention est également retrouvée de façon explicite dans la politique de vie privée de Dialogue.

Plusieurs organisations, comme Sentio Solutions et Bloom, restent assez vagues quant à leurs pratiques de rétention et offrent un discours similaire à celui-ci, à quelques variations près :

> « Nous conserverons vos données personnelles aussi longtemps que nécessaire aux fins pour lesquelles elles ont été collectées. Pour déterminer la durée de conservation, nous prenons en compte différents critères, tels que le type de produits et services demandés ou fournis par vous, la possibilité de vous réinscrire à notre service et l'impact sur les services que nous vous fournissons si nous supprimons certaines informations vous concernant. Nous conserverons également vos données personnelles comme l'exigent les politiques de conservation applicables ou comme le permet la loi en vigueur » (Sentio Solutions Inc., 2020, traduction libre).

En plus d'adhérer à ce discours, certaines comme Behavioral Signal, LifeWorks et Peakon sont imprécises quant à ce qui arrive une fois ce délai écoulé. À l'instar de la politique de vie privée de Peakon, celle de Behavioral Signal (2020, traduction libre) stipule qu'« après ce délai, [elle] supprimera ou rendra anonymes [les] informations, ou si cela n'est pas possible, [elle les] entreposera en toute sécurité et [les] isolera jusqu'à ce que la suppression soit possible ». Il n'est pas clair dans quels contextes et pour quelles raisons les données sont anonymisées au lieu d'être supprimées. D'autres organisations comme Modern Health et DeepAffects n'offrent aucune mention quant à leur pratique de rétention des données personnelles dans leur politique de vie privée ou dans leurs conditions d'utilisation, mis à part le passage souligné plus haut tiré des conditions d'utilisation de Modern Health (2019, traduction libre) qui stipule : « Vous acceptez en outre que la société ait le droit, pendant et après la durée des présentes conditions, d'utiliser, de stocker, de transmettre, de distribuer, de modifier, de copier, d'afficher, d'accorder des sous-licences et de créer des œuvres dérivées des données anonymes et agrégées ».

Au niveau de la sécurité et de l'entreposage

Au niveau des mesures de sécurité prises pour protéger les données personnelles, la majorité des organisations ont le même discours générique dans lequel elles assurent aux utilisateurs :

> « Nous appliquons des mesures techniques, physiques et organisationnelles appropriées qui sont raisonnablement conçues pour protéger les données à caractère personnel contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés, accidentels ou illégaux, en particulier lorsque les données à caractère personnel sont transférées sur un réseau, et contre toute autre forme de traitement illégal. L'accès aux données à caractère personnel est limité aux destinataires autorisés, selon le principe du besoin d'en connaître. Nous maintenons un programme complet de sécurité des informations qui est proportionné aux risques associés au traitement. Le programme est continuellement adapté pour atténuer les risques opérationnels et pour assurer la protection des données à caractère personnel en tenant compte des pratiques acceptées par l'industrie. Nous utilisons également des mesures de sécurité renforcées (par exemple, le cryptage) lors du traitement de données personnelles sensibles. Cependant, le transfert de données personnelles par internet comporte ses propres risques inhérents et nous ne garantissons pas la sécurité de vos données transmises par internet. Vous effectuez un tel transfert à vos propres risques » (Sentio Solutions Inc., 2020, traduction libre).

Ce discours, à quelques variations près, est tenu par dix des douze organisations que présente ce *benchmark*. Il n'y a que My Possible Self et Dialogue qui nomment explicitement les différentes mesures qu'elles prennent pour assurer la sécurité des données personnelles des utilisateurs.

En ce qui a trait à l'entreposage des données, Moodmetric le fait à même le cellulaire de l'utilisateur. Elle offre une solution infonuagique à ses utilisateurs dans laquelle elle garde les identifiants séparés des données de mesures. Cette solution leur permet de conserver leurs données historiques et ne contient pas les informations entrées manuellement sur l'application. Dans cette condition, seulement une très petite quantité d'informations personnelles est accessible à l'organisation. Cependant, elle stipule clairement que cette solution est optionnelle et que les utilisateurs peuvent jouir de l'ensemble des bénéfices de l'application sans y adhérer tout en conservant l'ensemble des données sur leur cellulaire.

La plupart des organisations mentionnent que les données personnelles sont transférées, traitées et entreposées dans leur pays d'origine et quelques-unes, comme Modern Health, Affectiva et LifeWorks, précisent que les données personnelles peuvent possiblement être transférées et entreposées dans tout autre pays où se situent des partenaires et compagnies affiliées. De façon intéressante, même lorsqu'elles agissent dans leurs capacités de sous-traitant, DeepAffects n'assure pas la sécurité d'entreposage des données de ses clients, de même que Modern Health n'assure pas la sauvegarde des données utilisateurs. Il serait intéressant de voir ce que contiennent leurs contrats de traitement des données respectifs à cet égard.

Au niveau de l'utilisation des témoins

DeepAffects et Moodmetric sont les seules organisations de ce *benchmark* qui font une utilisation minimale des témoins. Effectivement, DeepAffects mentionne qu'elle n'utilise pas les témoins de suivi et qu'elle ne fournit aucun lien vers les sites de tiers. Moodmetric pour sa part mentionne qu'elle n'utilise pas les témoins personnellement, mais que son application pourrait contenir des cookies des tiers qui fournissent les codes et librairies qu'elle utilise.

Les autres organisations utilisent les témoins et autres technologies sous toutes leurs formes, mais diffèrent quant à leur niveau de transparence. Effectivement, Bloom ne fait que mentionner que le terme « traiter » implique le fait d'utiliser des témoins, mais reste muette quant au genre de témoins qu'elle utilise, leur provenance, leur utilité et leur expiration. Certaines organisations, comme Behavioral Signal, offrent une page dédiée à leur politique de témoins sans pour autant offrir les détails mentionnés plus haut. D'autres, comme Affectiva et Modern Health dédient une petite partie de leur politique de confidentialité à l'utilisation de ces témoins et n'en fournissent qu'une brève explication.

Les plus transparents, comme Peakon, Sentio Solutions et My Possible Self, offrent une liste complète de leurs témoins qui contient leur utilité, leur provenance et leur expiration. Ces listes révèlent l'étendue de l'utilisation de ces témoins et un certain partage de données personnelles qui n'est pas toujours déclaré dans la section appropriée.

Finalement, sur les quelques organisations qui mentionnent la préférence Do Not Track, seulement quelques-unes la supportent. La majorité n'honore pas cette préférence, soit en raison de l'avancée rapide des technologies, comme le mentionne LifeWorks, ou encore parce qu'elles ne suivent pas les visiteurs de leur site pour leur fournir de la publicité de façon ciblée, comme le rapporte Modern Health. Cependant, ces explications ne sont pas toujours fournies.

Droits des utilisateurs

En ce qui a trait aux droits accordés aux utilisateurs, ceux-ci varient grandement d'une organisation à l'autre. Évidemment, les organisations comme Moodmetric, My Possible Self et Peakon qui se situent au sein de l'UE sont contraintes par la loi d'offrir au minimum les droits prévus par le RGPD à tous les utilisateurs de leurs services.

Les organisations nord-américaines ne sont pas régulées de façon aussi contraignante par les régulations relatives à la protection des données sur leurs territoires respectifs, mais doivent tout de même se plier au RGPD si elles comptent traiter les données d'utilisateurs résidant au sein de l'UE. À cet égard, les organisations adoptent des stratégies différentes. Certaines, comme Rise et Behavioral Signal offrent les droits prévus par le RGPD à tous leurs utilisateurs, et ce, peu importe leur pays d'origine, alors qu'Affectiva, Sentio Solutions et LifeWorks prévoient des droits différents pour les résidents de l'UE et de l'Angleterre qu'elles n'étendent pas aux résidents des autres territoires.

D'autres comme DeepAffects, Bloom et Modern Health, toutes trois logées aux États-Unis et faisant affaire à l'international, ne font aucune mention du RGPD ou encore du CCPA. DeepAffects fait allusion au Fair Information Principles qui sont des directives de bonnes pratiques relatives à la protection des données personnelles émises par le *Federal Trade Commission* (FTC) sur lesquelles elle semble se baser. Bloom ne fait que préciser que les utilisateurs peuvent la contacter s'ils veulent supprimer leurs données, alors que Modern Health ne mentionne que la possibilité pour le consommateur de modifier ses préférences marketing et de demander de modifier ou de supprimer ses données, tout en précisant qu'il est possible qu'elle ne puisse pas se plier aux demandes. L'absence d'allusion au RGPD manque de cohérence dans le cas de Modern

Health qui mentionne explicitement qu'elle se conforme au *Privacy Shield Framework* du FTC lui permettant de recevoir les transferts de données personnelles en provenance de l'UE et de la Suisse.

Dialogue, située au Canada et ne desservant que ce territoire, offre une très courte liste de droits limités et conditionnels qui répondent à la loi applicable au pays, mais est loin de se mesurer à celle prévue par le RGPD. Elle offre notamment le droit d'accès et de correction, avec plusieurs limitations qui sont largement décrites, ainsi que la possibilité de demander de supprimer des informations, qu'elle offre à sa discrétion.

Initiatives organisationnelles

Selon l'information disponible sur internet, très peu d'organisations sont dotées d'initiatives éthiques qui offrent un regard sur une culture et une vision qui supportent leurs pratiques en termes de gestion des données personnelles, autre que ce qu'offre leur politique de vie privée.

De toutes les organisations répertoriées dans ce *benchmark*, Behavioral Signal est la seule qui possède un code d'éthique. Ce code décrit les principes auxquels elle adhère, ses attentes envers tous les employés, l'environnement de travail dans lequel ceux-ci évoluent ainsi que les engagements qu'elle prend envers ses valeurs d'éthique, d'honnêteté, de transparence et de responsabilité. Le code n'est pas orienté vers les données personnelles en particulier, mais mentionne tout de même les informations personnelles de ses clients et l'importance qu'elle accorde à la façon dont elles sont manipulées ainsi que les attentes que l'organisation a envers ses employés à l'égard de celles-ci. L'organisation a mis en place différents mécanismes, comme le canal Speak Up, qui permettent aux employés de signaler leurs doutes à l'égard des comportements d'autres employés de façon confidentielle et sans crainte de réprimande. Le code demeure l'exemple le plus flagrant de l'engagement d'une compagnie envers l'éthique et de son désir de bâtir une culture de transparence et d'honnêteté qui gouverne les comportements des individus.

Pour sa part, Modern Health possède une politique de divulgation responsable qui incite toute personne croyant avoir détecté une vulnérabilité au niveau de la sécurité du site web ou de ses services d'en faire part à l'organisation qui s'engage à prendre les moyens pour « résoudre le

problème dans les cinq jours ouvrables suite à la divulgation » (Modern Life Inc., 2019, traduction libre). Elle possède également une page sur le statut de ses services qui montre l'état des services en temps réel et rapporte les incidents. Ces deux initiatives démontrent un effort de transparence ainsi qu'un engagement de la part de l'organisation envers la sécurité des données de ses utilisateurs.

Certaines organisations offrent une page dédiée à leurs valeurs et leurs pratiques, dont la pertinence est parfois questionnable dans la mesure où elles ne sont présentées que brièvement et ne sont appuyées par aucune action concrète, comme c'est le cas pour Affectiva. De son côté, Peakon possède une page qui décrit et illustre bien ses valeurs ainsi qu'une autre qui porte sur son engagement dans la diversité, l'équité et l'inclusion pour lequel elle produit des rapports annuels qui font état de son avancement et les stratégies qu'elles prévoient entreprendre pour s'améliorer. Finalement, Peakon est également investie dans ses responsabilités sociales et possède une page dédiée à son initiative Peakon for Good qui supporte des organisations philanthropiques à travers diverses activités.

3.4 Conclusion de l'analyse comparative des organisations

De toutes les entreprises rencontrées au travers des recherches effectuées pour réaliser ce *benchmark*, incluant celles qui n'ont pas été retenues, pratiquement aucune n'exploite la même technologie qu'EmoScienS. Celles qui le font, comme Affectiva, l'exploitent à des fins d'analytique média, de recherche, ou encore pour offrir des solutions destinées aux véhicules autonomes. Plusieurs autres organisations utilisent l'informatique affective, mais l'exploitent à travers la modalité vocale à l'instar de Behavioral Signal et DeepAffects. La majorité de ces solutions sont déployées en milieu organisationnel pour analyser la performance des employés, mais aucune de ces organisations ne se positionne clairement pour le bien-être et le développement de l'intelligence émotionnelle de ceux-ci à la façon d'EmoScienS. Les seules organisations pouvant être considérées comme compétiteurs directs, malgré qu'elles offrent des technologies de base complètement différentes, sont Moodmetric et Sentio Solutions.

Notre *benchmark* dépeint un portrait de l'industrie qui est loin d'être satisfaisant. Quoiqu'il révèle des informations tangibles et pertinentes à l'égard des pratiques de gestion des données

personnelles, ce sont souvent les subtilités et les non-dits qui se sont avérés les plus révélateurs. À l'issue de l'analyse, peu semble être réellement fait en termes d'éthique des données. Effectivement, le présent *benchmark* témoigne de nombreux exemples d'inconsistance, de manque de transparence et de dissimulation. Il révèle des choix questionnables, des apparences parfois trompeuses et dévoile de nombreuses zones grises qui laissent place aux interprétations, dont certaines sont lourdes de conséquences.

Cette conclusion est inquiétante pour les millions d'utilisateurs qui, pour la plupart, n'ont aucune conscience des risques auxquels ils sont exposés et des implications pour leurs droits et libertés. Par contre, cette conclusion implique également de nombreuses possibilités. L'état des lieux présenté par ce *benchmark* révèle une multitude d'opportunités pour EmoScienS et, espérons-le, plusieurs autres entreprises de se différencier et de se positionner au centre d'un mouvement qui ne fera que prendre de l'ampleur. Certes, tout reste à faire et les défis sont nombreux. Tout de même, la demande est présente et elle est pressante. Il n'en demeure qu'à ceux qui, à l'instar d'EmoScienS, veulent établir les nouvelles bases de l'industrie et saisir les opportunités qu'offre un champ qui, tout droit devant, est vaste et complètement libre.

4. IDENTIFICATION DES PRINCIPAUX ENJEUX ÉTHIQUES LIÉS AU DÉVELOPPEMENT DE LA TECHNOLOGIE D'EMOSCIENS

Suite à la revue de littérature et l'analyse de l'environnement présentés plus haut, certains enjeux semblent se démarquer pour EmoScienS. Nous croyons que ces enjeux sont ceux qui, à la lumière des aspirations éthiques de la startup ainsi que la technologie qu'elle exploite, auront des implications particulières pour celle-ci et nécessiteront de longues réflexions de la part de ses membres.

1. Ce rapport révèle certains compromis inhérents à la relation entre l'éthique et les intérêts commerciaux des organisations (Ekbia et al., 2015). Le marché actuel est peuplé d'organisations motivées par des intérêts qui dépassent largement la simple profitabilité et s'apparentent davantage à une « logique d'accumulation » sans fin à la Zuboff (2015, traduction libre : 74). Ces motivations laissent place à un ensemble de pratiques néfastes qui, face à d'énormes pressions concurrentielles et la nécessité de survivre, sont désormais la norme. Comment EmoScienS, une startup dont l'identité est ancrée dans l'éthique, peut aspirer tirer son épingle du jeu sans compromettre ses principes ? Alors que le sujet de l'éthique commence à être abordé sérieusement dans l'industrie, il est loin d'être une réalité. Effectivement, alors que le mouvement démarre lentement, EmoScienS devra certainement faire un exercice de positionnement stratégique pointilleux et cibler une clientèle susceptible de partager ses valeurs d'éthique.

2. À cet égard, quoi qu'intéressantes d'un point de vue commercial, les organisations privées possèdent des valeurs qui sont parfois plus nobles sur papier qu'en réalité. En plus d'être moins susceptibles d'être attirées par une startup qui respire l'éthique comme EmoScienS, ces organisations possèdent leurs propres intérêts qui sont souvent financiers. Le développement de relations d'affaires avec de telles organisations pourrait avoir des impacts sur l'identité de la startup ainsi que sa réputation. Effectivement, alors qu'elle n'aurait aucun contrôle sur l'utilisation secondaire des données et leurs impacts sur les individus visés comme la littérature le soulève, EmoScienS pourrait se retrouver à contribuer au phénomène qu'elle tente expressément de contrer.

3. Les nombreux remaniements légaux qui risquent d'influencer le terrain des organisations dans les prochaines années vont certainement engendrer la redéfinition de ce que signifie « être éthique » pour une organisation. Comme la loi est appelée à changer dans les prochaines années au Québec et au Canada, les organisations qui se disent éthiques et qui en font un élément phare de leur stratégie devront prévoir des façons d'aller au-delà des nouvelles dispositions. Effectivement, les standards d'éthique risquent de monter d'un cran alors que l'éthique deviendra la norme. Les organisations seront appelées à incarner leurs valeurs plus que jamais et à faire preuve d'ingéniosité et de créativité pour se démarquer. Alors que la revue de littérature a révélé l'inexistence du point de vue de l'utilisateur sans qui, de façon ironique, l'industrie s'écroule, il pourrait judicieux d'enfin le reconnaître à sa juste valeur. L'organisation qui aspire incarner l'éthique devrait considérer redonner à l'utilisateur une place de choix, une place à la hauteur de sa contribution, et collaborer avec ce dernier à toutes les étapes du développement de son approche éthique et du cycle de vie des données.

4. EmoScienS devra certainement accorder de longues réflexions à la question de la sécurité des données personnelles. Effectivement, alors que la startup se dit éthique, l'enjeu de confidentialité et de protection des données lui est particulièrement important en raison de la nature des données qu'elle collecte. Comme identifié dans la littérature, les techniques d'anonymisation actuelles ne sont pas suffisantes, mais plus encore, elles permettent quand même le ciblage, la manipulation et la surveillance. La question n'est pas sans conséquence pour la responsabilité et la profitabilité de l'entreprise. Effectivement, si les techniques d'anonymisation ne sont pas aussi efficaces que prétendu et qu'elles permettent la réidentification des individus, où réside la responsabilité de la startup qui, alors qu'elle se dit éthique, partage des données qui possèdent ce risque? Comment justifier l'adoption de cette pratique? Encore une fois, l'éthique et les intérêts commerciaux sont en équilibre précaire.

5. Pour la population générale, la technologie qu'EmoScienS exploite peut facilement être méprise pour de la reconnaissance faciale. Alors que le manque de connaissances, de

compréhension et de conscientisation à l'égard des technologies d'intelligence artificielle et de l'industrie du Big Data a été largement exposé dans la revue de littérature, la startup devra faire des efforts marketing considérables pour se distancier à tout prix de cette technologie qui suscite mécontentement palpable actuellement. Le positionnement de la startup doit être clair, ses communications transparentes et accessibles, sans quoi elle pourrait devenir victime de l'incompréhension du public et de la mauvaise réputation que s'est créée la reconnaissance faciale.

6. Finalement, nous croyons que la startup devra porter une attention particulière à l'impact qu'elle a sur ses utilisateurs. De par leur incompréhension et leur manque de connaissances, les utilisateurs se retrouvent en position de vulnérabilité face aux organisations qui, elles, détiennent une expertise qui les place en position d'autorité. Nous croyons que cette relation pourrait aller à l'encontre même de l'objectif d'EmoScienS d'accompagner les individus dans le développement de leur intelligence émotionnelle. Effectivement, la startup doit s'assurer qu'elle ne force aucune conclusion auprès des utilisateurs et qu'elle offre la possibilité pour celui-ci de valider ce que la technologie conclue. Plusieurs des utilisateurs futurs de sa technologie ont réellement besoin d'une aide à ce niveau et, de par cette faiblesse, sont plus susceptibles de ne pas reconnaître les instances où la technologie pourrait faire fausse route et leur renvoyer un profil émotionnel auquel ils ne s'identifient pas. Effectivement, la startup devra prendre des moyens concrets pour s'assurer que sa technologie n'exploite pas les vulnérabilités que sa technologie tente d'adresser.

5. APPRENTISSAGES

Ce projet représente pour moi l'immersion totale dans un domaine qui, à peine huit mois derrière, m'était complètement inconnu. Effectivement, provenant du domaine du développement organisationnel, la froideur qui émane de domaines techniques comme l'intelligence artificielle et la science des données me semblaient aux antipodes des valeurs humaines que ma spécialisation prône. J'ai eu ici l'occasion de confronter mes perceptions qui se sont rapidement révélées fausses alors que j'avançais dans mes recherches. Effectivement, ce projet m'a permis de me plonger dans un univers qui s'est révélé encore plus grand que ce qu'il n'avait l'air, mais surtout, totalement réconciliable avec mon domaine d'étude.

S'il y a bien une chose que mon cheminement en développement organisationnel et mon passage à HEC m'ont appris, c'est l'importance de l'interdisciplinarité et de la pluridisciplinarité, ce que le domaine de l'intelligence artificielle s'est révélé être au plus haut point. Effectivement, alors qu'il m'apparaissait principalement technique au début, les allures du domaine dissimulaient des dimensions humaine, philosophique, managériale, économique, politique et juridique, toutes d'une importance capitale pour la question à l'étude. Pour bien comprendre la gravité des enjeux et réaliser mon mandat, j'ai dû me plonger dans des sources philosophiques, légales, économiques et politiques qui n'avaient absolument rien à voir avec mon domaine d'expertise. J'ai alors compris toute l'importance de la perspective systémique qui nous est constamment rappelée et qui est considérée comme cruciale en développement organisationnel. Effectivement, la question que j'ai décidée d'attaquer pour la réalisation de ce projet m'a forcé à emprunter différentes perspectives pour, d'une part comprendre l'essence de la question et d'autre part, comprendre les enjeux qu'elle soulève. À travers ce balayage des différentes perspectives, j'ai acquis des connaissances primordiales qui m'ont permis d'approfondir ma compréhension du sujet à l'étude.

Mon parcours à la maîtrise m'a fait réaliser qu'en tant que société, nous construisons des structures beaucoup plus grandes que nous dont les forces défient complétement notre compréhension. Maintenant, dans ce tableau, l'être humain tend à être recalé au second plan, voire complétement évincé de la réflexion. Effectivement, il est souvent considéré comme un moyen d'enrichissement et un instrument primordial au bon fonctionnement d'une société qui n'a que très rarement ses

besoins et ses aspirations en tête, ce que ce projet n'a que confirmé. Effectivement, mes recherches m'ont fait découvrir un monde des affaires profondément déshumanisé et déshumanisant, en besoin criant de gens qui se soucient du bien-être des consommateurs. Elles m'ont révélé une industrie dont l'ampleur est si grande que les individus perdent de vue l'impact humain et tangible de leurs décisions. Elles m'ont révélée une industrie au-delà des technologies qu'elle développe, a besoin d'être gérée différemment, et surtout, plus humainement.

Le fait de réaliser ce projet en collaboration avec une *startup* aux aspirations éthiques m'a permis de me frotter d'un peu plus près aux milieux des affaires et d'observer les différents éléments qu'une entreprise qui pénètre dans cette industrie doit considérer. Son intérêt particulier pour l'éthique a révélé des tensions très intéressantes entre ses valeurs humaines et ses intérêts commerciaux. Effectivement, ces tensions vont nécessiter une certaine créativité qui, avant tout, nécessitera de se plonger sérieusement dans l'environnement d'affaire pour y saisir les différentes opportunités et faire face aux contraintes. L'exercice m'a fait réaliser l'importance particulière de posséder des connaissances adéquates dans toutes les sphères de cet environnement ainsi que des compétences transversales qui permettent de les naviguer et de s'y adapter, desquelles dépend lourdement le succès de toute entreprise.

7. CONCLUSION

Le mandat confié par EmoScienS, décliné en deux axes complémentaires, nous a mené à explorer la question de l'éthique des données et de l'intelligence artificielle sous différents angles. Dans un premier temps, la revue de littérature nous a permis de recenser les différents enjeux éthiques que les pratiques de gestion des données personnelles et l'informatique affective soulèvent. Alors que la première section avait pour objectif de révéler les vraies couleurs d'une industrie qui, dans l'ombre, profite, manipule et exploite, la deuxième section nous a permis de faire lumière sur les différents enjeux relatifs à la gouvernance des données et de démentir les affirmations d'objectivité sur lesquelles elle assoie sa légitimité. La troisième section, concentrée sur l'informatique affective et les enjeux qui lui sont propres, nous a révélé les risques inhérents des technologies affectives qui, en plus d'interférer avec une composante fondamentale de notre humanité, nos émotions, le font avec l'appui d'une science lourdement critiquée. Dans son ensemble, cette revue de littérature nous a permis d'exposer les inquiétudes, les doutes et les craintes au grand jour, ainsi que de nous projeter dans un avenir complètement « datatifié » et possiblement orchestré qui a toutes les raisons de nous inquiéter (Cuckier et Mayer-Schoenberger, 2013, traduction libre : 29).

À son tour, l'analyse de l'environnement d'EmoScienS nous a permis de pénétrer l'écosystème afin de voir ce qui s'y passe concrètement. Pour sa part, l'analyse PESTEL nous a permis de dresser un portrait des nombreux événements à prévoir dans l'écosystème d'EmoScienS. De façon générale, cet environnement s'est avéré porteur de changements imminents qui, en plus de répondre à certaines inquiétudes mentionnées dans la revue de littérature, pourront assister EmoScienS dans son développement et lui seront favorables dans la réalisation de ses aspirations.

Finalement, l'analyse comparative des organisations de l'industrie, réalisée en fin de rapport, nous a permis de cibler les organisations qui font partie de l'environnement de la startup et de faire lumière sur leurs pratiques concrètes en matière de gestion des données personnelles. En plus d'avoir permis l'analyse tangible d'une partie des pratiques qui sont au cœur des enjeux soulevés dans la revue de littérature, cette analyse nous a offert un regard privilégié et particulièrement pointu sur l'environnement compétitif d'EmoScienS. Ce portrait devrait lui permettre d'identifier les pratiques dont elle souhaite se doter pour se distinguer face à ses compétiteurs.

Le présent projet n'a jamais eu l'ambition ou la prétention de répondre à la question « comment bénéficier de tout le potentiel de l'intelligence artificielle et du Big Data, sans compromettre la dignité humaine au passage? » posée en introduction. Cependant, à l'issu de ce rapport, il semble évident que la confiance fasse partie de la réponse. Effectivement, la persistance de l'enjeu de confiance à travers les sections de ce document ne peut qu'illustrer son importance pour la suite des choses.

Maintenant, comment faire pour la gagner? Il est clair que la situation actuelle exige mouvements et changements, et ce, rapidement. Comme nous ne pouvons attendre les réponses aux nombreuses questions que portent les années à venir, nous nous devons d'entamer, quoique d'un pas incertain, les changements nécessaires. Pour EmoScienS, cela signifie certainement de s'attarder aux différents enjeux spécifiques et réflexions présentés plus haut. Loin de constituer des panacées à toutes les questions que soulèvent ce document et toutes celles qu'il nous reste à découvrir, ces pistes de réflexion et d'action pourront sans aucun doute l'aider à démarrer le bal et façonner le monde qui nous attend.

RÉFÉRENCES

« Le discours du Trône » (2020, 26 septembre). *La Presse*, section Débats. Récupéré de https://www.lapresse.ca/debats/courrier-des-lecteurs/2020-09-26/le-discours-du-trone.php

« The world's most valuable resource is no longer oil, but data » (2017, 5 mai). *The Economist*, section Leaders. Récupéré de https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Affectiva, Inc. (2020). *Privacy policy*. Récupéré de https://www.affectiva.com/privacy-policy/

Andrejevic, Mark (2014). « Big Data, Big Questions: The Big Data Divide », *International Journal of Communication*, vol. 8, pp.1673–1689.

Andrejevic, Mark et Kate Gates (2014). « Editorial. Big Data Surveillance: Introduction », *Surveillance & Society,* vol. 12, no 2, p. 185-196.

Angwin, Julia, Jeff Larson, Surya Mattu et Lauren Kirchner (2016). *Machine Bias*, ProPublica. Récupéré le 27 octobre 2020 de https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bannister, Catherine et Deborah Golden (2020). *Ethical technology and trust,* Deloitte. Récupéré le (date) de https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/ethical-technology-and-brand-trust.html

Barocas, Solon et Helen Nissembaum (2014). « Big Data's End Run Around Anonymity and Consent », dans *Privacy, Big Data and the Public Good: Framworks for Engagement*, Cambridge University Press, p. 44-75.

Basso, Tania, Roberta Matsunaga, Regina Moraes et Nuno Antunes (2016). « Challenges on Anonymity, Privacy and Big Data », communication présentée dans *2016 Seventh Latin-American Symposium on Dependable Computing (LADC),* IEEE.

Beavers, Anthony F. et Justin P. Slattery (2017). « On the Moral Implications and Restrictions Surrounding Affective Computing », dans *Emotions and Affect in Human Factors and Human-Computer Interaction*, Elsevier, p. 143-161.

Behavioral Signal Technologies, Inc. (2020). *Privacy policy*. Récupéré de https://behavioralsignals.com/legal/privacy-policy/

Bordeleau, Stéphane (2020). *Ottawa dépose un projet de loi pour protéger la vie privée des consommateurs*, Radio-Canada. Récupéré le 20 novembre 2020 de https://ici.radio-canada.ca/nouvelle/1750240/projet-loi-protection-vie-privee-ottawa

Boyd, Dana et Kate Crawford (2012). « CRITICAL QUESTIONS FOR BIG DATA », *Information, Communication and Society*, vol. 15, no 5, p. 662-679.

Breidbach, Christoph F. et Paul Maglio (2020). « Accountable algorithms? The ethical implications of data-driven business models », *Journal of Service Management*.

Breidbach, Christophe F., Michael Davern, Graeme Shanks et Ida Asadi-Someh (2019). « On the Ethical Implications of Big Data in Service Systems », dans *Handbook of Service Science, Volumme II*, Springer, p. 661-674.

Brigham, Tara J. (2017). « Merging Technology and Emotions: Introduction to Affective Computing », *Medical Reference Services Quarterly*, vol. 36, no 4, p. 399-407.

Bullington, Joseph (2005). « 'Affective' computing and emotion recognition systems: The future of biometric surveillance? », communication présentée au *InfoSecCD05: 2nd annual conference on Information security curriculum*, Kennesaw Georgia, Septembre.

Cadwalladr, Carole et Emma Graham-Harrison (2018, 17 mai). « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian,* section The Cambridge Analytica files. Récupéré de

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Calo, Ryan (2014). « Digital Market Manipulation », *The George Washington Law Review*, vol. 82, no 4, pp. 995-1051.

Castets-Renard, Émilie Guiraud et Jacinthe Avril-Gagnon (2020). *Rapport sur le cadre juridique applicable à l'utilisation de la reconnaissance faciale*, rapport, Observatoire international sur les impacts sociétaux de l'IA et du numérique. Récupéré de https://www.docdroid.com/YIDTjrr/cadre-juridique-applicable-a-lutilisation-de-la-reconnaissance-faciale-par-les-forces-de-police-dans-lespace-public-au-quebec-et-au-canada-pdf

Chen, Hsinchun, Roger H. L. Chiang et Veda C. Storey (2012). « Business Intelligence and Analytics: From Big Data to Big Impact », *MIS Quarterly*, vol. 36, no 4, p. 1165-1188.

Coeckelbergh, Mark (2020). *AI Ethics*, The MIT Press. The MIT Press Essential Knowledge Series, 229 p.

Commission d'accès à l'information (2020). *Guide d'accompagnement – Biométrie : principes à respecter et obligations légales des organisations*. Récupéré de https://www.cai.gouv.qc.ca/documents/CAI_G_biometrie_principes-application.pdf

Commission Européenne (2016). *Règlement général sur la protection des données*. RGPD. Récupéré de https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679#d1e1884-1-1

Cowie, Roddy (2012). « The Good Our Field Can Hope To Do, The Harm It Should Avoid », *IEEE Transactions on Affective Computing*, vol. 3, no 4.

Cowie, Roddy (2015). « Ethical Issues in Affective Computing », dans Sidney D'Mello (dir.), Jonathan Gratch (dir.) et Arvid Kappas (dir.) *The Oxford Handbook on Affective Computing*, Oxford University Press, pp. 334-348.

Crawford, Kate, Kate Milner et Mary L. Gray (2014). « Critiquing Big Data: Politics, Ethics, Epistemology », *International Journal of Communication*, vol. 8, pp. 1663-1672.

Crête, Mylène (2020, 03 novembre). « 100 millions de plus pour la santé mentale », *Le Devoir*, section Politique. Récupéré de https://www.ledevoir.com/politique/quebec/588934/annonce-en-sante-mentale-de-lionel-carmant

Cukier, Kenneth et Viktor Mayer-Schoenberger (2013). « The rise of big data: How it's changing the way we think about the world », *Foreign Affair.*, vol. *92*, p. 28.

Daily, Shaundra B., Melva T. James, David Cherry, John J. Porter III, Shelby S. Darnell, Joseph Isaac *et al.* (2017). « Affective Computing: Historical Foundations, Current Applications, and Future Trends » dans *Emotions and Affect in Human Factors and Human-Computer Interaction*, Elsevier, p. 213–231.

Daugherty, Paul, Marc Carrel-Billiard et Michael Biltz (2020). *Technology trends 2020: We, the post-digital people,* rapport, Accenture. Récupéré de https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-2/Accenture-Technology-Vision-2020-Full-Report.pdf

De Mauro, Andrea, Marco Greco et Michele Grimaldi (2015). « What is big data? A consensual definition and a review of key research topics », In *AIP conference proceedings*, vol. 1644, no 1, p. 97-104.

Deschamps, Tara (2020, 27 octobre). « Des dirigeants du domaine technologique s'adressent à Justin Trudeau », *La Presse*, section Techno. Récupéré de https://www.lapresse.ca/affaires/techno/2020-10-27/creation-d-un-plan-de-prosperite/des-dirigeants-du-domaine-technologique-s-adressent-a-justin-trudeau.php

Desjardins, François (2019, 11 décembre). « Fuite de données chez Desjardins : 1,8 millions de détenteurs de cartes de crédit touchés », *Le Devoir,* section Économie. Récupéré de

https://www.ledevoir.com/economie/568794/vol-de-donnees-chez-desjardins-1-8-million-de-detenteurs-de-cartes-de-credit-touches

Dialogue Technologies Inc. (202). *Privacy policy*. Récupéré de https://www.dialogue.co/en/privacy

Duffy, Brian R. (2008). « Fundamental Issues in Affective Intelligent Social Machines », *The Open Artificial Intelligence Journal*, vol. 2, p. 21-34.

Ekbia, Hamid, Michael Mattioli, Inna Kouper, G. Arave, Ali Ghazinejad, Timothy Bowman, Venkata Ratandeep Suri, Andrew Tsou, Scott Weingart et Cassidy R. Sugimoto (2015). « Big Data, Bigger Dilemmas: A Critical Rewiew », *Joural of the association for information science and technology*, vol. 66, no 8, pp. 1523-1545.

Feldman Barrett, Lisa, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez et Seth D. Pollak (2019). « Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements », *Psychological Science in the Public Interest*, vol. 20, no 1, p. 1-68.

Floridi, Luciano (2006). « The ontological interpretation of informational privacy », *Ethics and Information Technology*, pp. 1-16.

Floridi, Luciano (2014). « Open Data, Data Protection, and Group Privacy », *Philosophy and Technology*, vol. 27, p. 1-3.

Floridi, Luciano et Mariarosaria Taddeo (2016). « What is data ethics? », *Philosophical Transactions of The Royal Society A*.

Giguère, Ugo (2020, 8 novembre). « Les PME étouffent sous le poids de leurs assurances », *La Presse*, section PME. Récupéré de https://www.lapresse.ca/affaires/pme/2020-11-08/covid-19/les-pme-etouffent-sous-le-poids-de-leurs-assurances.php

González Fuster, Gloria (2010). « Inaccuracy as a privacy-enhancing tool », *Ethics and Information Tehcnology*, vol. 12, p. 87-96.

Gouvernement du Canada (2019). *Principales statistiques relatives aux petites entreprises – Janvier 2019*. Récupéré le 27 octobre de https://www.ic.gc.ca/eic/site/061.nsf/fra/h_03090.html

Gow, Glenn (2020, 21 août). « Environmental Sustainability And AI », *Forbes.* Récupéré de https://www.forbes.com/sites/glenngow/2020/08/21/environmental-sustainability-and-ai/?sh=4f09d9557db3

Hand, David J. (2018). « Aspects of Data Ethics in a Changing World: Where Are We Now? », *Big Data*, vol. 6, no 3.

Impératif de l'IA au Canada : Point critique pour la politique publique (2019b). Rapport, Deloitte. Récupéré de https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-point-critique-pour-la-politique-publique-aoda-fr-updated.pdf?location=top

Impératif de l'IA au Canada : Surmonter les risques, instaurer la confiance (2019). Rapport, Deloitte. Récupéré de https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-overcoming-risks-building-trust-aoda-fr-updated.pdf?location=top

Innovation, Sciences et Développement Économique Canada (2019). *Mandat du Conseil consultatif en matière d'intelligence artificielle du gouvernement du Canada*. Récupéré de http://www.ic.gc.ca/eic/site/132.nsf/fra/00003.html

Innovation, Sciences et Développement Économique Canada (2019b). *La Charte numérique du Canada en action : un plan par des Canadiens, pour des Canadiens.* Récupéré de https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00109.html

Innovation, Sciences et Développement Économique Canada (2020). *Charte canadienne du numérique : la confiance dans un monde numérique.* Récupéré de https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00108.html

Jehl, Laura, Alan Friel, Bakerhostetler LLP et *Practical Law Data Privacy Advisor* (2018). *CCPA and GDPR Comparison Chart*, Tableau comparatif, Thomson Reuters. Récupéré de https://www.info-hisa.si/wp-content/uploads/2019/11/CCPA-GDPR-Chart.pdf

Jolin-Barrette, Simon (2020). *Projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Assemblée nationale du Québec. Récupéré le 13 octobre 2020 de http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

Kokolakis, Spyros (2017). « Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon », *Computers & Security*, no 64, p. 122-134.

Kung, Johnny, Gaga Boskovic et Charlotte Stix (2020). *L'ère de l'IA : rapport sur les stratégiques nationales et régionales en matière d'IA deuxième édition*, rapport, CIFAR. Récupéré de https://www.cifar.ca/fr/ia/lere-de-l-ia-deuxieme-edition

Landowska, Agnieszka (2019). « Uncertainty in emotion recognition »*, Journal of Information, Communication and Ethics in Society*, vol. 17, no 3, p. 273-291.

Langlais, Kathy (2020). *Covid-19 : Le télétravail, une pratique qui est là pour de bon*, Raymond Chabot Grant Thornton. Récupéré le 7 octobre 2020 de https://www.rcgt.com/fr/nos-conseils/teletravail-apres-covid-19/

Lauzon, Véronique (2020, 10 octobre). « Une saison à haut risque », *La Presse*, section Covid-19. Récupéré de https://www.lapresse.ca/covid-19/2020-10-10/sante-mentale-et-pandemie/une-saison-a-haut-risque.php

Leduc, Daniel, Kathleen Houlihan, Heather Cameron, Margaret McConnell, Joshua Sadovnik et Stéphane Erickson (2020). *Surveiller les employés à distance: regard sur les technologies et considérations juridiques connexes liées au télétravail,* Norton Rose Fulbright. Récupéré le 7 octobre 2020 de https://www.nortonrosefulbright.com/fr-ca/centre-du-

savoir/publications/77b629db/surveiller-les-employes-a-distance-regard-sur-les-technologies-et-considerations-juridiques-connexes-lies-au-teletravail

Lessard, Frédérique-Emmanuelle (2016). *Enquête sur la santé psychologique étudiante*, FAÉCUM. Récupéré le 13 octobre 2020 de http://www.faecum.qc.ca/ressources/documentation/avis-memoires-recherches-et-positions-1/enquete-sur-la-sante-psychologique-etudiante

Lévesque, Lia (2020, 27 octobre). « Boulet dépose sa réforme attendue en santé-sécurité au travail », *La Presse,* section Affaires. Récupéré de https://www.lapresse.ca/affaires/2020-10-27/boulet-depose-sa-reforme-attendue-en-sante-securite-au-travail.php

LifeWorks Canada Ltd (2020). *Privacy policy*. Récupéré de https://www.lifeworks.com/ca/fr/portee/

Mai, Jens-Erik (2016). « Big Data Privacy: The datafication of personal information », *The Information Society*, vol. 32, no 3, p. 192-199.

Martin, Kirsten E. (2015). « Ethical Issues in the Big Data Industry », *MIS Quarterly Executive*, vol. 14, no 2, p. 67-85.

McStay Andrew et Lachlan Urquhart (2019). « 'This time with feeling?' assessing EU data governance implications of out of home appraisal based emotional AI », *First Monday*, vol 24, no 10. Récupéré de https://firstmonday.org/ojs/index.php/fm/article/view/9457/8146

McStay, Andrew (2016). « Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy) », *Big Data & Society*, p. 1–11.

McStay, Andrew (2020). « Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy », *Big Data & Society*, p. 1-12.

Meemo Media, Inc. (2020). *Privacy policy.* Récupéré de https://www.enjoybloom.com/privacy

Ministère du Travail, de l'Emploi et de la Solidarité Sociale (2020). *Projet de loi modernisation le régime de santé et de sécurité du travail – Le ministre Jean Boulet dépose un projet de loi visant à réformer le régime de santé et de sécurité du travail,* Gouvernement du Québec. Récupéré le [date] de https://www.quebec.ca/nouvelles/actualites/details/projet-de-loi-modernisant-le-regime-de-sante-et-de-securite-du-travail-le-ministre-jean-boulet-depos/

Modern Life Inc. (2019). *Privacy policy.* Récupéré de https://www.joinmodernhealth.com/privacy-policy

Morgan, Charles S., Karine Joizil, Mireille Trottier, Karl Bherer et Ellen Yifan Chen (2020). *Projet de loi 64 : Le gouvernement du Québec entreprend une réforme importante du régime de protection des renseignements personnels,* McCarthy Tétrault. Récupéré le 13 octobre 2020 de https://www.mccarthy.ca/fr/references/blogues/techlex/projet-de-loi-64-le-gouvernement-du-quebec-entreprend-une-reforme-importante-du-regime-de-protection-des-renseignements-personnels

My Possible Self Limited (s.d.). *Privacy policy*. Récupéré de https://www.mypossibleself.com/privacy-policy/

Newell, Sue et Marco Marabelli (2015). « Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datafication' », *Journal of Strategic Information Systems*, no 24, p. 3-14.

Normand, François (2020, 7 octobre). « Covid-19 : une petite PME sur cinq ne changera pas ses pratiques », *Les Affaires*, section Général. Récupéré de https://www.lesaffaires.com/secteurs-d-activite/general/covid-19-une-petite-pme-sur-5-ne-changera-rien-a-ses-pratiques/620223

Olstrom, Amy L., Darima Fotheringham et Mary Jo Bitner (2019). « Customer Acceptance of AI in Service Encounters: Undertanding Antecedents and Consequences » dans *Handbook of Service Science, Volumme II*, Springer, p. 77 à 103.

Peakon ApS (s.d.). *Privacy policy.* Récupéré de https://peakon.com/us/privacy-policy/

Picard, Rosalind (1995). *Affective computing*, Rapport technique no 321, Cambridge, MIT Media Laboratory Perceptual Computing, Récupéré de http://www.macs.hw.ac.uk/~yjc32/project/ref-social%20media%20campaign/1995-affective%20computing.pdf

Picard, Rosalind (2003). « Affective computing: challenges », *International Journal of Human-Computer Studies*, vol. 59, pp. 55–64.

Picard, Rosalind et Jonathan Klein (2002). « Computers that recognise and respond to users emotions: theoretical and practical implications », *Interacting with Computers*, vol. 14, p. 141-169.

Plante, Caroline (2020, 30 octobre). « D'autres investissements à venir, promets Carmant », *La* Presse, section Santé. Récupéré de https://www.lapresse.ca/actualites/sante/2020-10-30/sante-mentale/d-autres-investissements-a-venir-promet-carmant.php

Protecting privacy in practice: the current use, development and limits of Privacy Enhancing Technologies in data analysis (2019). Rapport, The Royal Society. Récupéré de https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf?la=en-GB&hash=862C5DE7C8421CD36C105CAE8F812BD0

Recommandation du Conseil sur l'intelligence artificielle (2019). OECD/LEGAL/0449

Rettino-Parazelli, Karl (2019, 26 mars). « Des investissements publics en IA sans retombées garanties », *Le Devoir*, section Économie. Récupéré de https://www.ledevoir.com/economie/550654/intelligence-artificielle

Richards, Neil M. et Jonathan H. King (2014). « Big Data Ethics », *Wake Forest Law Review,* vol. 49, p. 393-432.

Richardson, Sharon (2020). « Affective computing in the modern workplace », *Business Information Reniew*, vol. 37, no 2, p. 78-85.

Richterich, Annika (2018). *The Big Data Agenda,* London: University of Westminster Press. Récupéré de https://library.oapen.org/bitstream/handle/20.500.12657/30155/649695.pdf?sequence=1

Rise, Inc. (s.d.). *Privacy policy*. Récupéré de https://www.risescience.com/privacy

Scassa, Teresa (2019). *Une stratégie des données pour le Canada : Nous avons besoin d'une stratégie de gestion des données qui soutient nos valeurs et encourage l'innovation*, rapport, Forum des politiques publiques. Récupéré de https://ppforum.ca/fr/publications/strategie-des-donnees-pour-le-canada/

Scheutz, Matthias (2012). « The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots », dans *Robots Ethics: The Ethical and Social Implications of Robotics*, MIT Press, p. 205-221.

SeerNet Technologies LLC. (2017). *Privacy policy.* Récupéré de https://deepaffects.com/privacy-policy/

Sentio Solutions Inc. (2020). *Privacy policy.* Récupéré de https://policies.myfeel.co/en/privacy-notice?_ga=2.42988709.1838505332.1606507703-1899678138.1604509567

Simonite, Tom (2020, 01 mai). « How Well Can Algorithms Recognize Your Masked Face », *Wired,* section Business. Récupéré de https://www.wired.com/story/algorithms-recognize-masked-face/

Someh, Ida, Michael Davern, Christophe F. Breidbach et Graeme Shanks (2019). « Ethical Issues in Big Data Analytics: A Stakeholder Perspective », *Communications of the Association for Information Systems*, vol 44, p. 718-747.

Spiekermann, Sarah, Alessandro Acquisiti, Rainer Böhme et Kai-Lung Hui (2015). « The challenges of personal data markets and privacy », *Electronic Markets*, no. 25, p. 161-167.

Steinert, Steffen et Orsolya Friedrich (2020). « Wired Emotions: Ethical Issues of Affective Brain-Computer Interfaces », *Science and Engineering Ethics,* vol. 26, p. 351-367.

Sullins, John P. (2012). « Robots, Love, and Sex: The Ethics of Building a Love Machine », *IEEE Transactions on Affective Computing*, vol. 3, no 4.

Thatcher, Jim (2014). « Living on Fumes: Digital Footprints, Data Fumes, and the Limitations of Spatial Big Data », *International Journal of Communication*, vol. 8, pp. 1765-1783.

Top Strategic Technology Trends for 2021 (2020). Rapport, Gartner. Récupéré de https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/

Université de Montréal (2018). Déclaration de Montréal pour un développement responsable de l'IA

Vigofere Oy (2020). *Privacy policy.* Récupéré de https://moodmetric.com/privacy-policy/

Wittes, Benjamin et Jodie C. Liu (2015). « The privacy paradox: The privacy benefits of privacy threats », *Center for Technology Innovation at Brookings*.

Wixom, Barbara H. et Jeanne W. Ross (2017). « How to monetize your data », *MITSloan Management Review*, vol. 58, no 3, p. 10-13.

Yang, Chaowei, Qunying Huang, Zhenlong Li, Kai Liu et Fei Hu (2017). « Big Data and cloud computing: innovation opportunities and challenges », *International Journal of Digital Earth*, vol. 10, no 1, p. 13-53.

Yonck, Richard (2020). *Heart of the machine: our future in a world of artificial emotional intelligence*, New York, Arcade Publishing. 312 p.

Zuboff, Shoshana (2015). « Big other: surveillance capitalism and the prospects of an information civilization », *Journal of Information Technology*, vol. 30, p. 75-89.

Zwitter, Andrej (2014). « Big Data Ethics », *Big Data & Society*, vol. 1, no 2, pp. 1-6.