Revue de droit de l'Université de Sherbrooke

RDUS

La question du droit dans la transformation numérique des administrations publiques

Daniel Mockle

Volume 49, numéro 2-3, 2019

URI : https://id.erudit.org/iderudit/1086481ar
DOI : https://doi.org/10.7202/1086481ar

Aller au sommaire du numéro

Éditeur(s)

Revue de Droit de l'Université de Sherbrooke

ISSN

0317-9656 (imprimé)
2561-7087 (numérique)

Découvrir la revue

Citer cet article

Mockle, D. (2019). La question du droit dans la transformation numérique des administrations publiques. *Revue de droit de l'Université de Sherbrooke*, *49*(2-3), 223–314. https://doi.org/10.7202/1086481ar

Résumé de l'article

Avec la volonté affichée d'offrir des services publics entièrement numériques, les autorités veulent mener à terme une évolution amorcée il y a plus de vingt ans. Le contexte a toutefois changé depuis la création du premier « gouvernement en ligne ». Le cadre administratif et juridique n'est plus le même compte tenu des enjeux liés à la protection des données, à la création d'une identité numérique, au recours à l'infonuagique publique, à l'utilisation de données biométriques ainsi qu'à l'usage grandissant des algorithmes dans des procédures administratives automatisées. Si ce sont surtout les dimensions techniques et administratives qui retiennent l'attention, le cadre juridique de cette transition numérique offre un net contraste pour le choix des instruments d'intervention. Les solutions retenues montrent l'attrait d'un modèle de gouvernance publique fondé sur des instruments de gestion et du droit souple au détriment de la législation. Compte tenu des impératifs grandissants de protection du public, le cadre législatif est néanmoins en pleine évolution, bien qu'il présente encore plusieurs lacunes, faute d'une véritable loi-cadre pour la transition numérique des administrations publiques.

La question du droit dans la transformation numérique des administrations publiques

par **Daniel MOCKLE**[*]

Avec la volonté affichée d'offrir des services publics entièrement numériques, les autorités veulent mener à terme une évolution amorcée il y a plus de vingt ans. Le contexte a toutefois changé depuis la création du premier « gouvernement en ligne ». Le cadre administratif et juridique n'est plus le même compte tenu des enjeux liés à la protection des données, à la création d'une identité numérique, au recours à l'infonuagique publique, à l'utilisation de données biométriques ainsi qu'à l'usage grandissant des algorithmes dans des procédures administratives automatisées. Si ce sont surtout les dimensions techniques et administratives qui retiennent l'attention, le cadre juridique de cette transition numérique offre un net contraste pour le choix des instruments d'intervention. Les solutions retenues montrent l'attrait d'un modèle de gouvernance publique fondé sur des instruments de gestion et du droit souple au détriment de la législation. Compte tenu des impératifs grandissants de protection du public, le cadre législatif est néanmoins en pleine évolution, bien qu'il présente encore plusieurs lacunes, faute d'une véritable loi-cadre pour la transition numérique des administrations publiques.

---

[*] Professeur associé, Département des sciences juridiques, Université du Québec à Montréal.

The current reforms in public administration are intended to be the culmination of the move to implement digital government. Those reforms were already informing the implementation process some twenty years ago. However, since the first «e-government», the context has undergone significant changes. The use of clouds, biometric data, as well as the increasing use of algorithms in automated procedures all raise the issue of data protection, both public and private. While the focus is on the technical and administrative dimensions of these changes, their legal framework remains problematic. The choice of legal instruments reveals a preference for soft law as a regulatory tool in preference to legislation. While this preference is standard in the field of public policy, it warrants nonetheless the enhanced protection of citizens' rights and makes the case for the use of robust legislation in the place of administrative instruments. Despite the increasing use of legislation, the absence of a framework law leaves many issues unresolved from a legal perspective.

SOMMAIRE

Introduction

Au Canada, la transition numérique des administrations publiques offre un net contraste pour le choix des instruments d'intervention. Si cette transition s'est d'abord amorcée par l'élaboration de politiques, de lignes directrices et de stratégies, elle s'est ensuite matérialisée par le recours à la législation. Pour la dimension législative, l'Ontario et le Québec ont adopté des lois spécifiques en 2019 et en 2020. L'Ontario pourrait, selon les apparences, revendiquer la première place avec la *Loi de 2019 pour des services simplifiés, accélérés et améliorés* (*Simpler, Faster, Better Services Act*)[1]. Le Québec suit de près avec l'adoption en octobre 2019 de la *Loi favorisant la transformation numérique de l'administration publique*[2], ainsi que la création en 2020 d'un organisme spécialisé en matière de technologies de l'information : Infrastructures technologiques Québec[3]. Il faut néanmoins reconnaître que le Québec a créé, dès 2011, la fonction de dirigeant principal de l'information[4], et que ce mouvement de réforme est antérieur à la période actuelle, comme le montre la *Loi concernant le cadre juridique des technologies de l'information*[5] qui remonte à 2001. Même si cette loi ne vise pas les administrations publiques, elle offre plusieurs balises. Malgré ce nouveau cadre législatif de 2019-2020, la transition numérique est déjà une réalité tangible puisque des sites électroniques offrent de l'information et des services suivant le principe du guichet unique[6].

---

1 *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, L.O. 2019, c. 7.

2 *Loi favorisant la transformation numérique de l'administration publique*, RLRQ, c. T-11.003.

3 *Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec*, L.Q. 2020, c. 2. Adoptée en février 2020, cette loi est en vigueur depuis juin 2020.

4 *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03, art. 6 (ci-après « *Loi sur la gouvernance et la gestion des ressources informationnelles* »).

5 *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1.

6 Pour quelques exemples : DONNÉES QUÉBEC, en ligne : < https://www.donneesquebec.ca/fr/ >; QUÉBEC.CA, en ligne : < https://www. quebec.ca >; QUÉBEC, « La Zone entreprise », en ligne : < https://www2.gouv.qc.ca/entreprises/portail/quebec/infosite?lang=fr&x=2091483350 >.

En comparaison, les autorités fédérales préfèrent une approche fondée sur des instruments de gestion, comme en témoignent la *Politique sur les services et le numérique* ainsi que la *Directive sur les services et le numérique*, en vigueur depuis le 1er avril 2020[7]. Les autorités fédérales, notamment le Conseil du Trésor, poursuivent une démarche qui se caractérisait déjà par des politiques et des directives, notamment la *Politique sur la gestion des technologies de l'information* qui remonte à 2007[8]. La seule exception date de 2000 avec la deuxième partie de la *Loi sur la protection des renseignements personnels et les documents électroniques*[9] adoptée pour régir l'utilisation de moyens électroniques au sein de l'administration fédérale. En permettant l'usage de moyens électroniques en remplacement du support papier, cette loi, par son esprit et ses finalités, est très éloignée de la transition qui fait désormais l'objet de politiques et de directives au niveau fédéral. Sur un plan plus général, celui du commerce électronique, les autorités fédérales sont moins réticentes afin de proposer un cadre législatif. La *Charte canadienne du numérique*

---

7 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services et le numérique*, Ottawa, 2020, en ligne : < https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603 >; SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Directive sur les services et le numérique*, Ottawa, 2020, en ligne : < https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601 >; Secrétariat du Conseil du trésor du Canada, *Directive sur la prise de décision automatisée*, Ottawa, 2019, en ligne : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592&section= html. Un plan stratégique est également consultable. Il énonce dix « normes numériques » qui correspondent à des « principes du bon fonctionnement du gouvernement numérique » : SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Plan stratégique des opérations numériques de 2018 à 2022*, Ottawa, 2018, en ligne : <https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plan-strategique-operations-numerique-2018-2022.html#ToC6>. Il remplace le *Plan stratégique de la gestion de l'information et de la technologie de l'information du Gouvernement du Canada de 2017-2021*, en ligne : < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/plan-strategique-gestion-information-technologie-information.html >.

8 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur la gestion des technologies de l'information*, Ottawa, 2007, en ligne : < https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12755 >.

9 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, art. 31 et suiv.

diffusée en 2019[10] a été suivie en novembre 2020 par le dépôt du projet de loi C-11 qui ne vise pas les institutions fédérales[11].

Pour l'objet de notre étude sur la transition numérique des administrations publiques, la place de la législation est loin d'être exclusive, même au Québec. Ces différences doivent être nuancées puisque l'Ontario et le Québec ont également recours à des politiques et à des approches stratégiques afin de compléter et de mettre en œuvre leur législation[12]. Ailleurs au Canada, le recours à la législation aux fins de transformation numérique n'est pas au programme. Si la Colombie-Britannique et le Nouveau-Brunswick ont élaboré des stratégies[13], l'Alberta a créé un organisme à cette fin[14]. Enfin, la transformation numérique peut être organisée suivant des prémisses énoncées dans une politique[15].

La transition numérique des administrations publiques constitue une réalité empirique dont les contours peuvent susciter des interrogations. Depuis déjà trois décennies, plusieurs catégories d'administrations

---

10 INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA, *Charte canadienne du numérique : la confiance dans un monde numérique*, Ottawa, 2019, en ligne : < https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00108.html >.

11 *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, Projet de loi C-11, 2e session, 43e législatrure, 69 Elisabeth II, 2020.

12 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, *Stratégie de transformation numérique gouvernementale 2019-2023*, Québec, 2019, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/Strategie_TNG.pdf >. Pour l'Ontario : GOUVERNEMENT DE L'ONTARIO, *Directive sur les données ouvertes de l'Ontario*, 2019, en ligne : < https://www.ontario.ca/fr/page/directive-sur-les-donnees-ouvertes-de-lontario >.

13 GOUVERNEMENT DE LA COLOMBIE-BRITANNIQUE, *BC Digital Government*, en ligne : < https://digital.gov.bc.ca/ >; GOUVERNEMENT DU NOUVEAU-BRUNSWICK, *Digital New Brunswick*, en ligne : < https://www2.gnb.ca/ content/gnb/en/corporate/promo/dnb.html >.

14 GOUVERNEMENT DE L'ALBERTA, *Alberta Digital Innovation Office*, en ligne : < https://www.alberta.ca/alberta-digital-innovation-office.aspx> .

15 GOUVERNEMENT DE TERRE-NEUVE-ET-LABRADOR, *Digital Government and Service NL*, en ligne : < https://www.gov.nl.ca/digitalgovernment/ >; GOUVERNEMENT DE LA NOUVELLE-ÉCOSSE, *Digital Nova Scotia*, en ligne : < https://digitalnovascotia.com >.

publiques (ministères et organismes publics, entreprises publiques, agences, établissements de santé, établissements d'enseignement, collectivités territoriales, personnes morales de droit public de divers types) ont amorcé un virage informatique de grande ampleur, tant pour leur propre fonctionnement que pour les relations avec le public. En dépit de ces acquis, le législateur a priorisé «la transformation numérique de l'administration publique»[16], ce qui laisse prévoir, à tout le moins, une nouvelle étape. La loi de 2019 a été surtout conçue en vue d'établir des règles plus précises pour les « projets en ressources informationnelles d'intérêt gouvernemental » dans la mesure où un cadre juridique plus général pour ce type de ressources remonte déjà à 2011[17]. Si cette loi reste silencieuse sur la nature exacte des fins recherchées par les autorités, notamment celles qui sont visées au Québec par le Conseil du trésor, la *Stratégie de transformation numérique* élaborée en 2019 dissipe toute ambiguïté[18]. L'objectif principal est de parvenir à une numérisation complète des services publics sur le fondement de la définition de l'expression « organisme public », telle qu'elle est définie dans la loi de 2011[19]. L'ambition affichée consiste à offrir des « services publics numériques de bout en bout », en particulier grâce à la « robotisation des opérations administratives manuelles et récurrentes » et par l'énoncé de six vecteurs d'accélération de la transformation numérique[20]. Pour l'Ontario, c'est la « Priorité au numérique[21] », qui comprend néanmoins une nuance, puisque « les services ne devraient pas être accessibles par voie numérique seulement[22] ». Pour les autorités fédérales, dès 2007, « le passage aux services électroniques devait être fait

16 *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2.

17 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4.

18 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, , préc., note 11.

19 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 2.

20 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, préc., note 11, p. 5 et 19 (vecteurs d'accélération).

21 GOUVERNEMENT DE L'ONTARIO, *Services numériques de l'Ontario*, en ligne : < https://www.ontario.ca/fr/page/services-numeriques-ontario >.

22 *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, art. 5 (1) al. 3.

progressivement[23] ». En dépit de leurs différences de conception, ces approches convergent par l'utilisation de la méthode « dite de liste » qui fait appel à des annexes ou à une définition pour y énumérer les divers types d'administration publique visés[24]. Si la thématique de la transformation numérique relève de l'élaboration des politiques publiques, ce que montre l'utilisation prépondérante de politiques et de stratégies, un infléchissement en faveur d'un cadre juridique est de plus en plus manifeste, spécialement au Québec.

Dans les documents élaborés par les autorités publiques, la transformation numérique offre l'image avenante de la rapidité, de la simplicité et de l'accessibilité. Plusieurs enjeux techniques et juridiques ne sont pas forcément répertoriés, ou à peine esquissés, par les autorités concernées dans ces approches de diffusion pour le grand public. Ces enjeux sont la protection des données, le recours à l'infonuagique publique, l'utilisation potentielle de données biométriques, l'automatisation croissante des procédures administratives relatives à des décisions, l'usage grandissant des algorithmes, la perspective de la justice prédictive, pour ne donner que quelques exemples. La question du droit apparaît ainsi sous plusieurs dimensions. S'il semble légitime de s'interroger sur la nature du cadre juridique aux fins de protection du public, le choix des instruments d'intervention s'avère tout aussi important. Le droit est-il en mesure d'apporter des réponses appropriées pour cette transition, et peut-on encore faire état de l'objet « droit » si les autorités utilisent, en tout ou en partie, des instruments de gestion? À toutes fins utiles, cette transition pourrait n'être que technique et administrative, ce qui permettrait de reléguer le droit au second plan, et parfois d'en faire l'économie, comme le font plusieurs provinces canadiennes et les autorités fédérales.

---

23 CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services*, Ottawa, 2007 (abrogée en 2020), en ligne : < https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=27916 >.

24 Des différences n'en subsistent pas moins puisque, dans le cas du Québec, la *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, offre une énumération qui renvoie aux annexes de la *Loi sur l'administration financière*, RLRQ, c. A-6.001, alors que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, offre un autre type d'énumération aux articles 3 à 7.

Sur ce point, le rôle contrasté de la législation dans cette transition montre une différence qui fait figure de passage obligé pour le droit du numérique. Cette divergence oppose, en réalité, ceux qui, parmi les acteurs publics et privés, préfèrent recourir à des instruments de gestion et au droit souple (*soft law*) par rapport à d'autres intervenants ou observateurs qui préconisent l'utilisation d'instruments plus classiques, notamment la législation et la réglementation sous forme de règlements. Pour l'essentiel, ce débat repose sur les difficultés inhérentes à la réglementation du numérique, des algorithmes et de la robotique, ce qui justifierait une approche fondée sur l'élaboration de principes et d'orientations, par opposition à des règles contraignantes d'origine législative ou réglementaire. Cette prudence serait motivée par le caractère trop évolutif du domaine, de même que par la nécessité d'obtenir un minimum de consensus vu le nombre et la diversité des acteurs en jeu. À l'inverse, plusieurs exigences de protection des usagers et des citoyens rendraient indispensable l'élaboration d'un cadre législatif ou réglementaire issu d'un droit national ou supranational. Après nombre d'années de négociation, le Parlement européen a adopté le 14 avril 2016 le *Règlement général sur la protection des données* (RGPD) : celui-ci est devenu directement applicable dans l'ensemble des 28 États membres de l'Union européenne le 25 mai 2018[25].

La transition numérique des administrations publiques reflète ainsi une polarisation entre deux approches. En insistant sur le nombre des acteurs, la première fait appel au cadre conceptuel de la gouvernance pour justifier des lignes directrices et des politiques (instruments souples), mais elle intègre également la terminologie et les instruments du nouveau management public, avec la gestion stratégique et la figure du client. La

25 *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, Journal officiel de l'Union européenne, L 119, 4 mai 2016, en ligne : < https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2016:119:TOC > (ci-après « RGPD »).

seconde privilégie la protection du public[26] et le contrôle des citoyens sur leurs données personnelles (approche retenue dans le RGPD), ce qui oriente le débat vers l'élaboration de nouvelles lois ou la modification du corpus législatif existant. Les premières publications sur la thématique du droit et de la gouvernance ont mis en lumière le recours accru à des formules de substitution à la réglementation classique issue de lois et de règlements[27]. Le cadre conceptuel de la gouvernance a aussi été proposé pour privilégier des solutions de rechange mieux adaptées à la spécificité du numérique[28]. Les exigences propres à la mondialisation offrent une autre piste explicative[29]. Le recours à « des instruments de droit souple et dépourvus de tout effet juridique », notamment par l'élaboration de chartes, est largement préconisé en matière d'intelligence artificielle[30]. Si l'usage du droit souple est très répandu, la législation ne perd pas pour autant son rôle traditionnel afin de protéger correctement le public. Cette évolution contribue à accentuer une polarisation connue en droit public entre la figure

---

26 Si la *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, fait état de « mise à la disposition du public » pour les données ouvertes, elle vise, par son préambule, à rendre les services plus accessibles « à la population, aux collectivités et aux entreprises de l'Ontario ». Au Québec, la *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2, art. 1, cherche « à promouvoir la confiance du public ».

27 Valérie LASSERRE, *Le nouvel ordre juridique. Le droit de la gouvernance*, Paris, LexisNexis, 2015, p. 349 (« Du droit souple au droit de la gouvernance »); Daniel MOCKLE, *La gouvernance, le droit et l'État*, Bruxelles, Bruylant, 2007, p. 107 (outils de gouvernance, mécanismes de substitution, normes de rechange).

28 Luca BELLI, *De la gouvernance à la régulation de l'Internet*, Paris, Berger-Levrault, 2016, partie 2 (« La gouvernance mondiale de l'Internet »), p. 219; Danièle BOURCIER, « Comment s'accorder sur les normes? Le Droit et la Gouvernance face à Internet », (2006) 10-3 *Lex Electronica* 1; Michael E. MILAKOVICH, *Digital Governance. New Technologies for Improving Public Services and Participation*, Londres/New York, Routledge, 2011, chap. 1 (« The Transition from Electronic Government to Digital Governance »), p. 3; Stéphane BERNATCHEZ, « De la démocratie par le droit à la dictature des algorithmes? La théorie juridique à l'ère cybernétique », (2020) 25-3 *Lex Electronica* 10, 28 (La théorie du droit de la gouvernance).

29 Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation*, 2e éd., Montréal, Éditions Thémis, 2015.

30 Arnaud SÉE, « La régulation des algorithmes : un nouveau modèle de globalisation? », (2019) 5 *Revue française de droit administratif* 830, 836.

de la loi et un modèle de gouvernance fondé sur l'utilisation de politiques et de lignes directrices.

Devant cette alternative dans le choix des instruments, les autorités publiques sont loin d'être isolées, puisque l'actualité récente, marquée par des fuites de données dans des fichiers publics, par la croissance et la disponibilité des technologies de reconnaissance faciale, par le profilage ainsi que par l'accès à des données biométriques, a contribué à alerter l'opinion publique qui réclame des balises juridiques. Cette pression en faveur du droit risque, à court terme, d'infléchir substantiellement le contenu des politiques publiques, avec la réaffirmation de questions récurrentes. Quel est le cadre juridique approprié? Faut-il légiférer? Quel équilibre doit-on atteindre entre l'innovation technique et la protection du public?

Si ces interrogations revêtaient une réelle acuité en 2019, elles présentent désormais une valeur ajoutée dans le contexte de la pandémie de COVID-19 de 2020. Les conditions imposées à la population par l'urgence sanitaire ont favorisé l'accélération de ce processus de transition numérique pour toutes les organisations de nature publique ou privée. Certes, la pandémie a eu l'effet d'un catalyseur pour la dématérialisation du travail, et pour les relations avec les diverses catégories du public (citoyens, justiciables, clients des entreprises), mais elle a fait surgir également des enjeux technologiques qui relèvent du droit du numérique.

Pour limiter la propagation du virus, des moyens inédits ont été proposés[31]. Dans le but d'éviter un confinement trop sévère de leur population, plusieurs États occidentaux se sont montrés désireux de suivre

31 Pour une recension plus exhaustive de ces moyens, voir : Alexandra BAHARY-DIONNE et Karine GENTELET, *Les angles morts des réponses technologiques à la pandémie de COVID-19 : Disjonction entre les inégalités en santé et numériques structurantes de la marginalisation de certaines populations*, Ottawa, Observatoire international sur les impacts sociétaux de l'IA et du numérique, 2020, p. 23 (Les technologies numériques développées en réponse à la Covid-19).

l'exemple de quelques pays asiatiques[32], en autorisant l'implantation d'une application de traçage dans les téléphones intelligents. Le 29 mai 2020, la France a franchi cette étape pour les applications Contact Covid et SI-DEP (à ne pas confondre avec StopCovid)[33]. Au Canada, les autorités fédérales (Santé Canada) offrent depuis juillet 2020 la possibilité d'utiliser, sur une base volontaire, l'application Alerte COVID qui repose sur la technologie Bluetooth[34]. Au Québec, en mai 2020, plusieurs ministères avaient donné leur aval pour ce dispositif de traçage qui pourrait être mis en œuvre sur une base volontaire[35]. Réunie en août 2020, la Commission des institutions de l'Assemblée nationale avait recommandé d'éviter de se servir de cette technologie compte tenu des réserves importantes émises par les experts sur l'efficacité réelle de ces moyens, les vulnérabilités de la technologie Bluetooth, ainsi que sur l'inadéquation du cadre juridique[36]. En dépit de ces réserves, les autorités québécoises ont finalement décidé d'avoir recours à

32 En plus du code QR qui est affiché sur le téléphone intelligent, les autorités chinoises ont ajouté la reconnaissance faciale pour authentifier le porteur du code. Même en faisant exception de la Chine, « la Corée du Sud, Taïwan et Hong Kong ont eu recours à des moyens particulièrement intrusifs comme la géolocalisation, l'agrégation de nombreuses bases de données, voire le bracelet électronique» : Eugénie MÉRIEAU, « Le covid-19 en Asie orientale : Corée du Sud, Hong Kong, Japon, Singapour, Taïwan », (2020) 4 *Revue française de droit administratif* 695, 699.

33 *Décret nº 2020-650 du 29 mai 2020 relatif au traitement de données dénommé StopCovid*, (2020) 0131 J.O.R.F., texte nº 17.

34 Bernard BARBEAU, « L'application Alerte COVID est en ligne », *Radio-Canada*, 31 juillet 2020, en ligne : < https://ici.radio-canada.ca/nouvelle/1723570/application-tracage-covid-19-coronavirus-ottawa >.

35 Karim BENESSAIEH, « Traçage de la COVID-19 : une application québécoise prête en quelques semaines », *La Presse*, 20 juillet 2020, en ligne : < https://www.lapresse.ca/affaires/techno/2020-07-20/tracage-de-la-covid-19-une-application-quebecoise-prete-en-quelques-semaines.php >.

36 COMMISSION DES INSTITUTIONS, ASSEMBLÉE NATIONALE DU QUÉBEC, *Rapport – Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19*, Québec, 14 août 2020, en ligne : < http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-42-1/index.html#documentsReflexion >.

l'application Alerte COVID en septembre 2020[37]. Cette avancée technique a été ainsi réalisée sans modification du cadre législatif.

Ces dimensions montrent que la transition numérique des administrations publiques ne soulève pas que des enjeux organisationnels et institutionnels, mais qu'elle est susceptible également d'infléchir substantiellement les modalités de l'action publique. Sur le plan chronologique, il est inévitable que l'innovation technologique précède le droit. Cependant, sous réserve de ce constat, le choix d'un cadre juridique et des instruments d'action ne peut que réactualiser les questions récurrentes pour le droit du numérique. Si l'intervention du législateur est requise, faut-il modifier à la pièce des lois préexistantes ou prévoir la nécessité d'une loi plus générale de transition numérique? Malgré le fait que notre étude ait pour objet l'évolution du droit au Canada, et de façon plus précise ce qui a été réalisé au Québec, des perspectives de droit comparé s'avèrent essentielles afin de mesurer ce que font les Américains et les Européens dans ce domaine.

I. Le cadre juridique de la transition numérique

Pour la vaste majorité des États occidentaux, la première transition numérique correspond au « moment 2000 ». Les premières années du XXIe siècle correspondent en effet à la reconversion électronique des administrations publiques afin d'offrir le « gouvernement en ligne » (*e-administration*/*e-governement*). Cet impératif avant tout technologique devait promouvoir l'efficience et la qualité des services publics[38]. La Conférence internationale de Copenhague en 2005 a permis de réunir une

37 Le Québec est devenu ainsi la cinquième province qui utilise ce dispositif après l'Ontario, le Nouveau-Brunswick, la Saskatchewan, Terre-Neuve-et-Labrador ainsi que le Manitoba.

38 Organisation de coopération et de développement économiques (OCDE), *L'administration électronique : un impératif*, Paris, Études de l'OCDE, 2004, p. 29; Edwin LAU, « Principaux enjeux de l'administration électronique dans les pays membres de l'Organisation de coopération et de développement économiques (OCDE) », (2004) 110 *Revue française d'administration publique* 225.

trentaine de textes sur le sujet où la question du droit reste peu étudiée[39]. Dans les publications de cette période, le droit semble peu pertinent, à la lumière d'un cadre conceptuel qui a pour objet la réforme de l'État[40]. Au Canada, le droit n'était pas encore un élément de réflexion pour le développement de l'État électronique[41]. L'orientation consumériste était visible dans les réflexions générales[42]. Dans une perspective élargie, qui dépasse les limites du droit canadien, l'ouvrage dirigé par Georges Chatillon et Bertrand du Marais a néanmoins été une exception notable en incluant plusieurs enjeux juridiques[43].

La première transition peut paraître éloignée de celle qui a cours actuellement[44]. Il y a vingt ans, la terminologie de l'intelligence artificielle,

---

39 Maria A. WIMMER et autres (dir.), *Electronic Government*, Linz, Springer-Verlag Berlin Heidelberg, 2009; Maria A. WIMMER et autres (dir.), *Electronic Government*, Copenhagen, Springer-Verlag Berlin Heidelberg, 2005.

40 Hsinchun CHEN et autres (dir.), *Digital Government. E-Government Research, Case Studies, and Implementation*, New York, Springer US, 2008; Michael BÖHLEN et autres (dir.), *E-Governement: Towards Electronic Democracy*, Bolzano, Springer-Verlag Berlin Heidelberg, 2005; Francis JUBERT, Elizabeth MONTFORT et Robert STAKOWSKI (dir.), *La e-administration. Levier de la réforme de l'État*, Paris, Dunod, 2005; Ake GRÖNLUND, *Electronic Government: Design, Applications and Management*, Hershey, Idea Group Publishing, 2002, p. 23.

41 Voir le cadre conceptuel proposé par Sandford BORINS et autres (dir.), *Digital State at the Leading Edge*, Toronto, University of Toronto Press, 2007, p. 14 (« Conceptual Framework »). Pour un premier bilan de cette période, voir Daniel MOCKLE, « La virtualité et l'État de droit », dans Karim BENYEKHLEF et Pierre TRUDEL, *État de droit et virtualité*, Montréal, Éditions Thémis, 2009, 9, à la p. 37.

42 John CLARKE et autres, *Creating Citizen-Consumers: Changing Publics & Changing Public Services*, Thousand Oaks, Sage Publications, 2007; Tae Hyun KIM, Kwang Hyuk IM et Sang Chan PARK, « Intelligent Measuring and Improving Model for Customer Satisfaction Level in e-Government », dans M.A. WIMMER et autres, *Electronic Government* (2005), préc., note 37, p. 38.

43 Georges CHATILLON et Bertrand DU MARAIS, *eGovernment for the Benefit of Citizens : proceedings from the Colloquium*, Bruxelles, Bruylant, 2004, partie 1 (« The Law applicable to eGovernment »).

44 Des nuances plus fines peuvent être proposées afin d'expliquer le déroulement chronologique de cette transition numérique : Tomasz JANOWSKI, « Digital Government Evolution: From Transformation to Contextualisation », (2015) 32 *Government Information Quaterly* 221 (évolution en quatre étapes).

des algorithmes, de l'infonuagique, des mégadonnées (*big data*), ainsi que celle de l'apprentissage automatique (*machine learning*) était peu répandue, voire encore inconnue pour quelques termes et concepts, notamment en droit[45]. La deuxième transition numérique apparaît plus ambitieuse par son objet et ses finalités[46]. Outre une numérisation complète et exhaustive des services publics aux fins de consultation et d'élaboration des politiques publiques, elle est également orientée vers l'ouverture des données publiques, l'accès sécurisé, la protection des données personnelles, dans le contexte du traitement algorithmique de grandes bases de données[47]. L'expression « gouvernement 3.0 » (*government 3.0*) a été proposée en 2017[48] pour marquer la transition par rapport au gouvernement 2.0 (*government 2.0*) dont l'usage découle du terme « Web 2.0 » (essor des médias sociaux)[49].

---

45 Tung-Hui HU, *A Prehistory of the Cloud*, Londres, MIT Press, 2015, chap. 4 (« Seeing the Cloud of Data »), p. 112 (« crossover between military practices and marketing practices»); Donald E. KNUTH, *Éléments pour une histoire de l'informatique*, Californie/Paris, Stanford University, CSLI Publications/Société mathématique de France, 2011, p. 363 (origine de l'expression «analyse des algorithmes»). En informatique, la première édition de l'ouvrage fondateur remonte à 1968 : Donald E. KNUTH, *Fundamental Algorithms*, Reading (MA), Addison-Wesley, 1968.

46 « For this cultural perception may well be the main divide between the first digital revolution, in the 1990s, and the second, in the 2010s » : Mario CARPO, *The Second Digital Turn: Design beyond Intelligence*, Cambridge (MA), Londres, The MIT Press, 2017, p. 18. Voir également M.E. MILAKOVICH, préc., note 27, p. 14 (« The Transition from Electronic Government to Digital Governance »).

47 Andrea KÖ et autres (dir.), *Electronic Government and the Information Systems Perspective*, 8e Conférence internationale, EGOVIS 2019, Linz, Springer, 2019, notamment les deux premières parties (« Open Data and Open Innovation » et « Data-Driven Approaches in e-Government »); Rob KITCHIN, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*, Thousand Oaks (CA), Sage, 2014, p. 114 (« Governing People »).

48 Adegboyega OJO et Jeremy C. MILLARD (dir.), *Government 3.0 – Next Generation Government Technology Infrastructure and Services*, Londres, Springer, 2017.

49 Soon Ae CHUN et autres, « Government 2.0: Making Connections between Citizens, Data and Government », (2010) 15-1 *Information Polity* 2 (Web 2.0 Technologies); Brian E. DIXON, « Towards E-Government 2.0: An Assessment of where E-Government 2.0 is and where it Is Headed », (2010) 15-2 *Public*

Cette transition met parfois en lumière des dimensions qui vont au-delà des administrations publiques. Comme le montre l'exemple de la France avec la *Loi pour une République numérique* (2016)[50], le législateur peut devenir plus ambitieux afin d'assurer la neutralité du Net, le droit au maintien de la connexion à Internet, l'accessibilité du numérique et la couverture numérique du territoire. À plus ou moins court terme, c'est la numérisation complète des relations du public avec toutes les catégories d'administrations publiques qui est visée[51], et la conséquence en sera l'informatisation des processus administratifs de demandes et de réclamations en fonction d'une identité numérique et d'accès sécurisés[52]. Il en résulte une mobilisation où la capacité technique des administrations publiques constitue le premier objet de réflexion[53]. La construction d'un modèle unifié apparaît comme l'une des principales préoccupations[54].

La deuxième transition pose avec plus d'acuité le problème récurrent du choix des instruments d'intervention. En droit administratif, le

Administration and Management 418; Daniel MINTZ, « Government 2.0 – Fact or Fiction », (2007-2008) 36-4 *Public Manager* 21. Pour l'analyse du rôle accru des internautes dans l'environnement du type Web 2.0, voir Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 30.

50 *Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique*, J.O. 8 octobre 2016.

51 Pour une perspective comparée (Danemark) : Jannick SCHOU et Morten HJELHOLT, *Digitalization and Public Sector Transformations*, Cham, Palgrave Macmillan, 2018. Pour repenser les notions d'espace et de territoire : Jannick SCHOU et Morten HJELHOT, « Digital State Spaces: State Rescaling and Advanced Digitalization », (2019) 7-4 *Territory, Politics, Governance* 438, 441 (« The Digital and the Spatial »).

52 Pour un recul temporel, voir Paul HENMAN, *Governing Electronically: E-Government and the Reconfiguration of Public Administration, Policy and Power*, Basingstoke (GB), Palgrave Macmillan, 2010, chap. 7 (« Reconfiguring Public Administration »), p. 115 et suiv.

53 Isaac Kofi MENSAH, « Impact of Government Capacity and E-government Performance on the Adoption of E-government Service », (2020) 43 *International Journal of Public Administration* 303.

54 Yogesh K. DWIVEDI et autres, « An Empirical Validation of a Unified Model of Electronic Government Adoption (UMEGA) », (2017) 34 *Government Information Quaterly* 211.

choix des formes d'action étatique représente une thématique connue, ne serait-ce que pour expliquer de nouvelles formes de réglementation, la mise en œuvre de techniques non réglementaires ou l'existence de formules de substitution du droit par le recours à des instruments de gestion[55]. Cette diversification des formes d'intervention de l'État peut également être justifiée à la lumière des travaux sur les « outils de gouvernance[56] ». La véritable ligne de partage n'en reste pas moins le choix de la législation et de la réglementation, par opposition à la vaste catégorie des formules de substitution. Rappelons, par exemple, que le Québec a conféré à la nouvelle gestion publique un cadre législatif, en adoptant en 2000, la *Loi sur l'administration publique*[57]. À titre comparatif, les autorités fédérales ont préféré une solution plus proprement politique et administrative avec la parution du rapport intitulé *Fonction publique 2000*[58]. En dépit de cette différence, notre analyse n'a pas pour objet de réintroduire des clichés à propos du rôle de la législation en monde de common law contrairement aux systèmes de tradition romaniste. Le droit américain offre un démenti à ce type de stéréotype puisque, en matière de nouvelle gestion publique, la *Government Performance and Results Act*[59] a été adoptée en 1993.

---

55 Daniel MOCKLE, « Politiques, directives et instruments de gestion », dans JurisClasseur Québec, coll. « Droit public », *Droit administratif*, fasc. 5, Montréal, LexisNexis Canada, 2019 (LAd/QL); Daniel MOCKLE, « L'évincement du droit par l'invention de son double : les mécanismes néo-réglementaires en droit public », (2003) 44 *C. de D.* 297; Pierre ISSALYS, *Répartir les normes. Le choix entre les formes d'action étatique*, Québec, Société de l'assurance automobile du Québec, 2002; Daniel MOCKLE, « Gouverner sans le droit? Mutation des normes et nouveaux modes de régulation », (2002) 43 *C. de D.* 143.

56 Pearl ELIADIS, Margaret M. HILL et Michael HOWLETT (dir.), *Designing Government. From Instruments to Governance*, Montréal/Kingston, McGill/Queen's University Press, 2005; Pierre LASCOUMES et Patrick LE GALÈS, *Gouverner par les instruments*, Paris, Presses de Sciences Po, 2005; Lester M. SALOMON (dir.), *The Tools of Government. A Guide to the New Governance*, Oxford, Oxford University Press, 2002.

57 *Loi sur l'administration publique*, L.R.Q. c. A-6.01.

58 GOUVERNEMENT DU CANADA, *Fonction publique 2000. Guide de la gestion du changement dans la Fonction publique : les voies de l'innovation*, Ottawa, Approvisionnements et Services Canada, 1990.

59 *Government Performance and Results Act*, 31 U.S.C., § 20, (1993).

À l'échelle canadienne, la polarisation se situe davantage entre une culture de gestion fondée sur l'utilisation de lignes directrices et de politiques en regard des impératifs de légitimité fondés sur le recours à la loi. En filigrane, c'est le poids politique et juridique du Conseil du Trésor qui se révèle souvent déterminant, puisqu'au niveau fédéral ses nombreuses interventions puisent principalement leur fondement dans la *Loi sur la gestion des finances publiques*[60]. Dans la perspective de la transition numérique, cette culture peut être confortée par deux influences. La première est britannique, compte tenu de la mise en œuvre, depuis 2012, de la stratégie *Digital by Default*[61], laquelle permet de faire l'économie d'une loi de transition numérique. Cette approche est répandue au sein des États du Commonwealth, comme en témoignent les stratégies élaborées en Australie[62] et en Nouvelle-Zélande[63]. La seconde reflète à maints égards l'utilisation des mécanismes du droit souple, ainsi que la place souvent déterminante de procédés administratifs (qui ne sont pas des instruments juridiques) dans ce qui peut paraître comme un processus plus général de substitution de la législation aux fins de transition numérique. Cette dimension est importante compte tenu de l'association du droit mou (*soft law*) à plusieurs champs du numérique.

---

60 *Loi sur la gestion des finances publiques*, L.R.C. 1985, c. F-11, art. 7 (1) a). Le Conseil du Trésor peut agir au nom du gouvernement fédéral pour définir « les grandes orientations applicables à l'administration publique fédérale ».

61 GOUVERNEMENT DU ROYAUME-UNI, CABINET OFFICE, *Government Digital Strategy*, Londres, 2012, en ligne : < https://www.gov.uk/government/publications/government-digital-strategy >.

62 GOUVERNEMENT AUSTRALIEN, *Vision 2025. Digital Transformation Strategy*, Canberra, Digital Transformation Agency, 2018, en ligne : < https://www.dta.gov.au/digital-transformation-strategy >. La Commission du service public, de concert avec l'agence responsable de la transition numérique, a produit un autre document en 2020 : Australian Public Service Commission / Digital Transformation Agency, *APS Digital Professional Stream Strategy*, 2020, en ligne : https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-professional-stream-strategy.pdf.

63 GOUVERNEMENT DE NOUVELLE-ZÉLANDE, *Strategy for a Digital Public Service*, en ligne : < https://www.digital.govt.nz/digital-government/strategy/strategy-summary/strategy-for-a-digital-public-service/ >.

A) Les débats contemporains sur le choix des instruments

Dans une perspective générale, les débats contemporains sur l'intelligence artificielle, la robotique, le numérique et la gouvernance d'Internet ouvrent des perspectives pour le choix des instruments. La thématique liée à Internet est riche d'enseignements pour le mode d'intervention, ainsi que le choix de l'autorité compétente, même si la dimension internationale reste prépondérante. Pour la réglementation et la gouvernance requise par la mise en œuvre d'Internet, le nombre de propositions reflète la variété des intervenants. Si plusieurs documents ont été élaborés par des personnes engagées dans la tenue de conférences scientifiques ou par des groupes de recherche, d'autres émanent d'organisations internationales comme l'Unesco, l'Organisation de coopération et de développement économiques (OCDE) ou le Conseil de l'Europe. En 2015, l'Unesco a publié une analyse chronologique comparative de 52 déclarations, lignes directrices et principes[64]. Bien que la majorité de ces documents apparaissent sous forme de déclarations, comme la *Déclaration de Paris*[65] de 2014, ainsi que la *Déclaration africaine des droits et des libertés de l'Internet*[66] adoptée la même année, moins nombreux sont ceux qui ont été élaborés sous forme de chartes[67], de

64 Rolf H. WEBER, *Principes de la gouvernance de l'Internet, Analyse comparative*, Paris, Unesco, 2015, p. 25 et suiv., en ligne : < https://unesdoc.unesco.org/ark:/48223/pf0000235370 >.

65 UNESCO, *Déclaration de Paris*, 5 mai 2014, en ligne : < https://en.unesco.org/sites/default/files/wpfd_2014_statement_final.pdf >, présentée à l'occasion de la Conférence internationale pour la Journée mondiale de la liberté de presse (organisée par l'Unesco) par des experts des médias et des libertés publiques.

66 *Déclaration africaine des droits et des libertés de l'Internet,* Association pour le progrès des communications (APC), 28 août 2014, en ligne : < https://www.apc.org/fr/project/securiser-les-droits-de-lhomme-en-ligne-en-afrique-par-le-biais-dun-reseau-fort-et-actif-de >.

67 *Charte des droits de l'Internet*, Association pour le progrès des communications (APC), 2001 (révisée en 2006), en ligne : < https://www.apc.org/fr/pubs/charte-des-droits-dinternet >; Grégor BRANDY et Vincent MANILÈVE, « Charte mondiale des droits sur Internet », *Slate FR*, 6 novembre 2015*,* en ligne : < http://www.slate.fr/story/109205/charte-mondiale-droits-internet >.

principes[68], de codes d'éthique[69] ou de recommandations[70]. Malgré cette diversité, à la différence des traités, « ils ne sont pas juridiquement contraignants », car ils offrent, de façon générale, des recommandations et des principes. En revanche, les textes élaborés par les organisations internationales compétentes en cette matière ont une portée beaucoup plus grande sur leurs États membres[71]. Il faut surtout retenir de cette évolution la place prépondérante des principes[72] même si, par ailleurs, des droits sont revendiqués pour les usagers d'Internet.

Il existe encore peu d'instruments plus classiques au niveau national ou supranational. À titre d'exemple, le Brésil a adopté une loi en 2014 qui concerne de façon spécifique l'usage d'Internet[73]. Le but principal de cette loi est l'élaboration de principes, de garanties, de droits et de devoirs pour l'usage d'Internet au Brésil. L'article 3 énumère de nombreux principes, tandis que l'article 7 offre une liste de droits et de garanties pour les usagers. Cependant, comme en témoigne le dernier Forum sur la gouvernance d'Internet (tenu à Berlin, en 2019), les initiatives strictement nationales sont critiquées dans le but d'inclure tous les acteurs intéressés[74].

---

68 IEEE STANDARDS UNIVERSITY, « Open Standard Principles », 1er novembre 2012, en ligne : < https://www.standardsuniversity.org/article/open-standards-principles/ >; OCDE, *Recommandations du Conseil sur les principes pour l'élaboration des politiques de l'Internet*, 2011, en ligne : < https://legalinstruments.oecd.org/public/doc/270/270.fr.pdf >.

69 *Code d'éthique pour la société de l'information proposé par le Conseil intergouvernemental du programme information pour tous*, Paris, Unesco, Conférence générale, 36e sess., 2011, en ligne : < https://unesdoc.unesco.org/ark:/48223/pf0000212696_fre >.

70 OCDE, préc., note 68.

71 R. WEBER, préc., note 64, p. 84 (« Valeur normative des documents »).

72 Le rôle prépondérant des principes a été signalé par Pierre TRUDEL, « État de droit et E-Gouvernement », dans K. BENYEKHLEF et P. TRUDEL, préc., note 41, 373, 387 (« Un droit exprimé sous la forme de principes directeurs »).

73 *Marco Civil da Internet*, Loi no 12 965 du 23 avril 2014. Pour la présentation de cette loi (avec traduction vers l'anglais), on consultera le document suivant : CHAMBER OF DEPUTIES, *The Brazilian Civil Framework of the Internet*, Brasilia, 2016.

74 À l'occasion de cette rencontre, l'UNESCO, *Steering AI and Advanced ICTS for Knowledge Societies, A Rights, Openness, Access and Multi-stakeholder*

La loi brésilienne met toutefois en lumière ce qui apparaît comme le véritable enjeu de l'usage d'Internet et, par extension, des réseaux numériques qui lui sont associés : la protection des données nominatives des usagers et, de façon plus générale, le droit à la confidentialité des communications, sans oublier le droit à la vie privée. C'est à la lumière de ces dimensions qu'il faut comprendre l'élaboration du RGPD de l'Union européenne[75], en vigueur depuis le 25 mai 2018. Dans sa version définitive du 27 avril 2016, ce règlement est l'aboutissement de quatre années de délibération[76]. Contrairement aux directives, les règlements sont directement applicables dans l'ensemble des 28 États membres, et ne requièrent pas une loi de transposition pour ce faire, ce qui signifie désormais qu'il y a un seul ensemble de règles relatives à la protection des données pour l'Union européenne. Les entreprises non européennes sont également soumises au RGPD lorsqu'elles proposent des biens et des services à des résidents européens ou qu'elles visent ces derniers par le profilage[77]. Le RGPD offre aux citoyens de l'Union européenne un contrôle accru sur leurs données privées, notamment pour l'acceptation des témoins (*cookies*) sur les sites Web et l'utilisation qui est faite des données transmises par les internautes (consentement explicite). À l'article 17, le RGPD crée en outre un droit à l'effacement des données à caractère personnel sur demande de la personne intéressée (version allégée du droit à l'oubli). La question sensible du « profilage[78] » fait l'objet d'une disposition spécifique (art. 22) en interdisant toute décision fondée sur un traitement automatisé, si cette dernière a des effets juridiques sur une personne ou se

Perspective, Berlin, 2019, p. 120*,* affirme en conclusion dans cette étude : « it is important to note that a purely national and unilateral decision-making at the level of principles, norms, rules, and policies can be potentially detrimental to rights, openness and access pillars discussed in this publication » .

75 Le sigle GDPR, issu de la version anglaise *General Data Protection Regulation*, est très répandu.

76 RGPD, préc., note 25.

77 Le COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Le nouveau règlement sur la protection des données aura des répercussions sur les entreprises canadiennes », 22 février 2018, en ligne : < https://www.priv.gc.ca/fr/nouvelles-du-«commissariat/nouvelles-et-annonces/2018/an_180222/ >, a commenté ces nouvelles obligations pour les entreprises canadiennes.

78 Le profilage est défini à l'article 4 du RGDP (« Définitions »).

trouve susceptible de la toucher « de manière significative de façon similaire ». Cette disposition est importante compte tenu d'enjeux qui relèvent plus précisément du droit administratif. Le RGPD définit aussi à l'article 25 le principe de protection des données dès la conception (*privacy by design*), dans le but de prévoir des exigences relatives à la protection des données personnelles dès la conception des produits, des services et des systèmes qui exploitent des données à caractère personnel. En outre, il établit une nouvelle règle, celle de la « sécurité par défaut », qui impose à toute organisation de disposer d'un système d'information sécurisé[79]. Enfin, l'article 37-1.a prévoit que la désignation d'un délégué à la protection des données est obligatoire lorsque le traitement des données est effectué par une autorité publique ou un organisme public, à l'exception des autorités qui exercent une fonction juridictionnelle (ce sont les différentes catégories de cours et de tribunaux).

En dépit de son applicabilité directe au sein des États membres de l'Union européenne, le RGPD a été complété à l'échelon national par des lois d'adaptation qui ont eu pour conséquence la modification de la législation antérieure. Ainsi, pour donner l'exemple de la France, la *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*[80] a été modifiée par la *Loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles*[81]. Tous les États membres de l'Union européenne ont fait ce suivi[82]. Le RGPD fait désormais figure de

79 Pour le traitement, la conservation et l'accessibilité des données à caractère personnel, des « mesures techniques et organisationnelles appropriées » doivent garantir que ces données ne seront pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique visée (art. 71 RGDP).

80 *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JORF du 7 janvier 1978, 227.

81 *Loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles*, JORF nº 0141 du 21 juin 2018.

82 La liste de ces lois nationales figure à l'annexe 2 de l'ouvrage d'Olivia TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, p. 415.

modèle, et son rayonnement international est incontestable[83]. À titre d'exemple, le Brésil a adopté sa propre version en août 2018[84]. Les autorités européennes veulent désormais franchir une autre étape avec l'élaboration d'une loi qui vise les plateformes numériques. À l'été 2020, la Commission européenne a mené une consultation sur ce projet (*Digital Services Act*)[85]. Dans une longue résolution rédigée sur le fondement de 31 considérants et de 89 principes, le Parlement européen a donné son appui en octobre 2020[86]. Cette évolution montre que des impératifs de protection favorisent l'élaboration d'un cadre législatif et réglementaire. Sur ce plan, les autorités européennes ne sont pas isolées, car la Californie a adopté en 2018 la *California Consumer Protection Act* (CCPA)[87] qui est en vigueur depuis le 1er janvier 2020 et qui concerne les informations personnelles utilisées par les grandes entreprises[88]. Pour l'essentiel, cette loi offre aux consommateurs le droit de savoir quel est le type d'information personnelle utilisée par

83 « Le RGPD à la conquête du monde », *Magazine Décideurs*, 22 mars 2019, en ligne : < https://www.magazine-decideurs.com/news/le-rgpd-a-la-conquete-du-monde >.

84 *Lei Geral de Proteçao¸de Dados Pessoais*, Lei nº 13.709/2018.

85 *Consultation on the Digital Services Act Package*, en ligne : < https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package >. Pour un commentaire, voir Florence G'SELL et Filippo LANCIERI, « Nouvelle législation européenne sur l'économie numérique : ce qu'on peut attendre du Digital Services Act », *Blog du Club des juristes*, 23 octobre 2020, en ligne : < https://blog.leclubdesjuristes.com/digital-services-act/ >.

86 *Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur la législation relative aux services numériques : améliorer le fonctionnement du marché unique*, 2020/2018(INL). La résolution comprend une annexe. D'autres résolutions ont été adoptées pour les services numériques et l'intelligence artificielle.

87 *California Consumer Privacy Act of 2018*, CAL. STAT. ch. 55 (2018) (ci-après « CCPA »).

88 Une entreprise est assujettie aux dispositions du CCPA, préc., note 87, art. 1798.140 (c) (1) (A), (B) et (C), si l'une des conditions suivantes est remplie : 1) elle a un revenu annuel supérieur à 25 millions de dollars américains; 2) elle achète ou vend de l'information personnelle provenant de plus de 50 000 consommateurs, familles, ménages et appareils électroniques; 3) elle tire plus de la moitié de ses revenus annuels de la vente d'informations personnelles.

l'entreprise[89], le droit à l'oubli numérique ou de supprimer des données personnelles (*right to delete personal information*) et le droit de retrait (*right to opt out*) par rapport aux entreprises qui vendent de l'information personnelle[90]. De plus, la CCPA reconnaît aux consommateurs qui se prévalent de ces droits la garantie de ne pas faire l'objet de discrimination sous forme d'exclusion, de diminution de service ou de tarification accrue. Pour sa part, l'État de Washington a manifesté son intention d'élaborer un cadre législatif comparable, mais en incluant également des mesures spécifiques pour les mécanismes de reconnaissance faciale[91].

Avec le dépôt en novembre 2020 du projet de loi C-11 relatif à la protection de la vie privée des consommateurs, le Canada a rompu avec sa réserve en proposant un premier cadre législatif susceptible de régir l'utilisation des renseignements personnels recueillis et utilisés aux fins du commerce électronique[92]. La partie 1 a notamment pour fonction de remplacer la première partie de la *Loi sur la protection des renseignements personnels et les documents électroniques* (laquelle aura dorénavant le titre de *Loi sur les documents électroniques*). La partie 2 précise le rôle du Commissaire à la protection de la vie privée tout en instituant un tribunal administratif (le Tribunal de la protection des renseignements personnels et des données) afin d'entendre les appels formés contre certaines décisions rendues par le Commissaire. La comparaison du cadre juridique offert par ce projet de loi avec celui du RGPD est une piste de réflexion qui dépasse le cadre de notre étude sur les administrations publiques. Si le projet de loi C-11 ne vise pas les institutions fédérales qui sont énumérés en annexe de la *Loi sur la protection des renseignements personnels*[93], en revanche, il n'est pas dénué de tout intérêt pour la divulgation de renseignements

89 Ce droit inclut l'accès aux finalités commerciales de la vente d'informations personnelles et l'accès aux catégories d'entreprises pour le partage de ces informations.

90 Pour ce type de requête, l'entreprise doit offrir sur son site WEB un lien de type « *Do not Sell my Info* ».

91 *Washington Privacy Act*, Bill S. 6281, 66th Leg., Sess. §1 (Wash., 2020). Ce projet de loi est encore en discussion au début de l'année 2021.

92 *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, Projet de loi C-11, préc., note 11.

93 *Id.*, par. 6 (4) a.

personnels à des administrations publiques. À condition que les renseignements personnels d'un individu soient dépersonnalisés[94], ils peuvent être communiqués à l'insu de la personne intéressée « à une institution gouvernementale au Canada » ou à d'autres établissements publics pour « une fin socialement bénéfique »[95]. De même, des renseignements personnels peuvent être communiqués, à l'insu ou sans le consentement d'un individu, à une institution gouvernementale pour l'application du droit fédéral ou provincial, notamment dans la perspective de contravention au droit[96].

Avec le dépôt du projet de loi 64 en juin 2020[97], le Québec a également manifesté sa volonté de modifier la loi relative à la protection des renseignements personnels dans le secteur privé[98]. En comparaison du cadre juridique proposé au niveau fédéral, sa démarche favorise davantage la protection des renseignements personnels que leur circulation.

Ces interventions législatives et réglementaires relatives à la protection des renseignements personnels au sein des entreprises n'ont pas pour objet direct la transition numérique des administrations publiques. Ainsi, la loi québécoise de 2019 cherche avant tout à prévoir « des règles applicables dans le cadre de la réalisation de projets en ressources informationnelles d'intérêt gouvernemental ». Si le législateur prend soin de rappeler le respect du droit à la vie privée et le principe de transparence, les renseignements personnels obtenus ne peuvent être utilisés qu'aux seules fins du projet en ressource informationnelle, ce qui exclut, *a priori*, la transmission de ces informations à des fins commerciales[99]. L'objectif

94 Le projet de loi ne fait pas de distinction entre la dépersonnalisation et l'anonymisation dans sa définition du terme « dépersonnaliser » à l'art. 2.

95 *Loi de 2020, Id.*, par. 39 (1).

96 *Id.*, art. 43 à 48.

97 Projet de loi no. 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, Première session, 42e législature, 12 juin 2020, arts. 93 et suiv.

98 *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1.

99 Sous réserve des normes relatives « aux données ouvertes » qui peuvent ainsi autoriser leur disponibilité pour le public, l'utilisation commerciale n'est pas

premier ne semble pas la protection du public au sens strict, mais davantage l'accessibilité des données et la confiance du public[100]. Ce n'est qu'avec le dépôt du projet de loi 64 que le Québec cherche à proposer un nouveau cadre juridique pour la protection des renseignements personnels dans le secteur public[101].

B) Le rôle de la législation

Malgré sa proximité géographique avec les États-Unis, le Canada a réalisé sa première transition numérique sans recours à une loi d'orientation. Dans cette première phase qui correspond au début de la décennie 2000[102], il n'existe pas de loi comparable à l'*E-Governement Act* de 2002[103]. Dans une période relativement courte (1999-2006), l'initiative dite du « Gouvernement en direct (GED) » a été réalisée au vu des objectifs fixés[104]. Lors de l'ouverture initiale du site Web du gouvernement du Canada (www.Canada.gc.ca) en 1995, des liens avaient été créés vers plus de 400 sites Web du gouvernement fédéral au détriment d'un effort de synthèse et d'accessibilité. La création d'un portail intégré et l'instauration de voies de communication protégée comme ePass, afin d'assurer un

exclue en Ontario : *Loi de 2019 pour des services simplifiés, accélérés et améliorés,* préc., note 1, art. 5 (2) al. 3.

100 Si la *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, fait état de « mise à la disposition du public » pour les données ouvertes, elle vise, par son préambule, à rendre les services plus accessibles « à la population, aux collectivités et aux entreprises de l'Ontario »; au Québec, l'article premier de la *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2, cherche « à promouvoir la confiance du public ».

101 Projet de loi no. 64, préc., note 97. Ce projet qui vise à modifier la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. c. A-2.1, est commenté plus loin dans ce texte.

102 David BROWN, « 2. The Government of Canada: Government On-Line and Citizen-Centred Service », (2016) *Digital State at the Leading Edge* 37.

103 *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899 (2002); 44 U.S.C. § 101. Cette loi inclut la *Federal Information Security Management Act of 2002*, qui correspond au titre lll, ainsi que la *Confidential Information Protection and Statistical Efficiency Act*, qui constitue le titre V.

104 GOUVERNEMENT DU CANADA, *Gouvernement en direct 2004*, Ottawa, Travaux publics et Services gouvernementaux Canada, 2004.

service sécuritaire de paiement en direct, ont permis au Canada d'être, au début du XXIe siècle, l'un des États les plus avancés dans la transformation électronique des services publics[105]. En revanche, celle-ci a été faite sans cadre législatif[106].

Durant cette période, l'Australie avait créé en 1997 un guichet unique, Centrelink, qui a été institué sous forme d'agence[107]. Le recul du temps montre néanmoins que l'*E-Government Act* de 2002 a été très novatrice en offrant un canevas qui sera suivi par plusieurs États. Aux fins du droit fédéral, les autorités américaines ont créé le poste de responsable en chef fédéral de l'information (*federal chief information officer*), qui s'occupe de l'ensemble des politiques pour la transformation électronique du gouvernement fédéral[108]. Même si ce haut fonctionnaire ne correspond pas à l'autorité de protection des données, telle qu'elle a été recommandée par le RGPD, il offre un modèle qui prévoit ce que le Canada propose désormais avec le dirigeant principal de l'information[109]. Sur le plan

105 En 2005, « Canada was ranked first by the Accenture consulting firm in its annual international survey of e-government service delivery » : D. BROWN, préc., note 91, p. 37. Les études contemporaines insistent davantage sur la progression numérique des États en fonction de plusieurs facteurs qui dépassent la numérisation des administrations publiques. En 2016, un rapport commandé par la Commission européenne classait la Finlande, la Suède, le Danemark, la Corée du Sud, les États-Unis et le Japon bons premiers : *International Digital Economy and Society Index (I-DESI)*, en ligne : < https://ec.europa.eu/digital-single-market/en/news/2016-i-desi-report >.

106 Ce constat avait déjà été fait par Karim BENYEKHLEF, « L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion », (2004) 110-2 *Revue française d'administration publique* 267, 275.

107 *Commonwealth Services Delivery Agency Act (1997)*, Acts of Parliament of the Commonwealth of Australia, No. 31 of 1997, art. 6.

108 Il a été désigné comme l'autorité responsable du nouveau bureau (Office of Electronic Government) au sein du ministère du Budget (Office of Management and Budget).

109 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services et le numérique*, préc., note 7, art. 4.3.

chronologique, c'est néanmoins la Corée du Sud qui peut revendiquer la première place en ayant élaboré dès 2001 l'*E-Government Act*[110].

La loi de 2002 énonce sept constats, auxquels s'ajoutent onze objectifs[111], avec une approche analogue à celle de la *Privacy Act* qui remonte à 1974[112]. Dans le premier titre (« Office of Management and Budget Electronic Government Services »), la loi de 2002 a permis de créer un conseil afin d'assister le responsable en chef de l'information (art. 3603)[113] et un fonds spécifique (E-Government Fund) à des fins budgétaires (art. 3604). Le deuxième titre (« Federal Management and Promotion of Electronic Government Services ») énumère les responsabilités attribuées aux agences fédérales en vue de la transition numérique. Il oblige ces dernières à tenir compte de l'existence des individus qui n'ont pas accès à Internet et à reconnaître la nécessité d'assurer l'accessibilité au réseau aux personnes souffrant de handicaps. Au sein de chaque agence, un poste de responsable en chef de l'information (*chief information officer*) est créé afin d'assurer l'application de la loi et pour faire rapport (*E-Government Status Report*). La loi règle la question de la compatibilité des méthodes acceptables afin de sécuriser les transactions électroniques avec le gouvernement. Elle pose notamment le principe de l'accès unique par un portail intégré (Federal Internet Portal), tout en réservant l'utilisation d'un site Web distinct pour les différentes cours fédérales[114].

---

110 Choong-Sik CHUNG et Sung-Bou KIM, « A Comparative Study of Digital Government Policies, Focusing on E-Government Acts in Korea and the United States », (2019) 8 *Electronics* 1362.

111 *E-Government Act of 2002*, préc., note 103, art. 2; 44 U.S.C. § 3601 (*Findings and Purposes*).

112 *Privacy Act of 1974*, 5 U.S.C. § 552a.

113 Parmi ses fonctions, ce conseil doit veiller, de concert avec le National Institute of Standards and Technology, à l'élaboration de recommandations pour la mise en œuvre de standards (*information technology standards*). Le législateur a été plus ambitieux dans la *Privacy Act of 1974*, préc., note 112, art. 5, en créant la Privacy Protection Study Commission, composée de sept membres (trois membres sont nommés par le président; deux membres le sont par le président du Sénat; et deux autres, par l'orateur (*speaker*) de la Chambre des représentants).

114 L'*E-Government Act of 2002*, préc., note 103, aborde également la gestion et la conservation des dossiers électroniques au sein des cours fédérales.

La loi de 2002 ne néglige pas la question sensible de l'accessibilité, de l'usage et de la préservation de l'information gouvernementale. À cette fin, elle crée un comité de coordination (Interagency Committee) entre les agences fédérales. Dans ce contexte, de nombreuses questions font l'objet de dispositions détaillées, notamment pour le classement des données, les modalités de leur accès, le type d'information que les agences doivent présenter sur leur site Web, ainsi que la création d'un répertoire des sites Web offerts par le gouvernement fédéral. Pour la confidentialité des données, la loi propose des nuances sous la rubrique de l'information sensible (*classified, sensitive or private information*). Elle oblige surtout les agences à faire des études d'impact (*privacy impact assessment*) et à afficher sur leur site Web le type de données recueillies, l'usage qui en est fait, la question du partage, la nature du consentement requis, de même que la sécurisation des données, le tout en conformité avec les dispositions de la *Privacy Act* de 1974[115]. Sur le plan chronologique, cette loi de 1974 est à l'origine de la règle *No Disclosure without Consent* (qui compte néanmoins 12 exceptions). Enfin, la loi de 2002 offre de nombreuses dispositions en vue de faciliter la circulation des spécialistes de l'informatique entre les secteurs public et privé, de déterminer des règles relatives aux contrats de type partenariat (*share-in-savings contracts*), ainsi que celles qui sont relatives à l'acquisition des technologies de l'information par les États et les collectivités locales. Enfin, la loi insiste sur la nécessité des protocoles communs pour faciliter l'échange d'information.

Le contenu très détaillé de la loi américaine de 2002 offre un net contraste avec le caractère empirique de l'approche canadienne durant cette période. Malgré l'usure du temps et l'apparition de nouveaux enjeux technologiques, la loi américaine offrait d'emblée un cadre général afin de poser des balises. Sur le plan législatif, le Canada a préféré remédier à certaines lacunes en créant Services partagés Canada (SPC) en 2012[116]. Même si la formulation de la *Loi sur Services partagés Canada* reste peu explicite quant aux enjeux numériques, les systèmes de technologie de

115 *Privacy Act of 1974*, préc., note 112.

116 *Loi sur Services partagés Canada*, L.C. 2012, c. 19. Pour améliorer et simplifier les services numériques de l'administration fédérale américaine, l'United States Digital Service a été créé le 11 août 2014 au sein du Bureau exécutif de la présidence américaine.

l'information offerts par SPC ont pour objet l'amélioration et l'uniformisation du traitement des données suivant des protocoles communs. La principale mission de SPC reste l'harmonisation du stockage de données pour éviter les problèmes de duplication entre chaque agence, organisme et ministère au niveau fédéral. SPC doit également veiller à la cybersécurité des systèmes et des réseaux au sein des ministères et des organismes fédéraux, ainsi qu'offrir des services infonuagiques[117].

Dans le même esprit, le Québec avait créé dès 2005 le Centre de services partagés afin de mettre à la disposition de la population, parmi de nombreux services, « des produits et services en matière de technologie de l'information et de télécommunication et en assurer la gestion et la maintenance[118] ». Par le dépôt du projet de loi nº 37 en septembre 2019, le Québec a préféré scinder cette mission générale en créant le Centre d'acquisitions gouvernementales pour l'offre de biens et services, tout en réservant à Infrastructures technologiques Québec un rôle de soutien afin d'assurer la transition numérique des organismes publics[119]. Ce nouvel organisme permet la concentration et le développement d'une expertise en matière d'infrastructures technologiques[120], et l'offre de services infonuagiques aux « organismes publics » tels qu'ils sont définis par l'article 2 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du*

117 Cette information est consultable en ligne : < https://www.canada.ca/fr/services-partages.html >.

118 *Loi sur le Centre de services partagés du Québec*, RLRQ, c. C-8.1.1., art. 5 (3). La portée de cette loi était restreinte aux organismes publics tels qu'ils sont définis par l'article 7 (annexe 1 de la *Loi sur l'administration financière*, préc., note 24), ainsi qu'aux organismes dont le personnel est nommé suivant la *Loi sur la fonction publique*, RLRQ, c. F-3.1.1.

119 *Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec*, projet de loi nº 37, (adoptée – 2020), 1re sess., 42e légis. (Qc); La *Loi sur le Centre de services partagés du Québec* est abrogée depuis.

120 À titre comparatif, la France avait créé en 2003 l'Agence pour le développement de l'administration électronique. Dès 2005, elle sera intégrée, au fil de diverses réformes, au sein de l'Administration centrale. Depuis octobre 2019, une direction interministérielle du numérique a été créée en étant toujours rattachée au Secrétariat général du Gouvernement.

gouvernement[121]. Cette loi a été rédigée de façon à assurer la prépondérance du Conseil du trésor dans la détermination des orientations et des priorités. À titre d'exemple, Infrastructures technologiques Québec peut fournir ses services à toute autre personne ou à toute autre entité désignée par le président du Conseil du trésor[122]. Cette loi énumère néanmoins des missions spécifiques qui concernent la prestation de services aux organismes publics[123]. Enfin, pour compléter ce tableau législatif, le Québec a suivi l'approche américaine de l'*E-Government Act* en créant, en 2011, la fonction de dirigeant principal de l'information au sein du Secrétariat du Conseil du trésor[124], de même que celle de dirigeant de l'information pour chaque ministère, et sur autorisation du Conseil du trésor, dans un organisme public[125].

Comme l'a fait le Québec, l'Ontario a institué un poste de directeur du numérique et des données[126], ce qui répond à l'exigence minimale de désignation d'un délégué à la protection des données (obligatoire pour toute autorité publique ou tout organisme public) prévue par le RGPD[127]. Ce directeur a la responsabilité d'élaborer des normes relatives aux services numériques et pour les données ouvertes[128]. Dans le cas des services numériques, ces normes « peuvent régir toute question », notamment les exigences liées aux programmes et à la prestation des services, ainsi que les

121 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4.

122 *Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec*, préc., note 3, art. 6 de la loi édictée par l'article 2 de la loi omnibus.

123 *Id.*, art. 4.

124 Le dirigeant principal de l'information a son propre site Web : en ligne : < https://www.tresor.gouv.qc.ca/ressources-informationnelles/dirigeante-principale-de-linformation/ >.

125 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 6 et 8.

126 *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, art. 3.

127 RGPD, préc., note 25, art. 37-1 a).

128 Pour ces normes, le directeur du numérique et des données reste soumis à l'approbation du Conseil de gestion du gouvernement; *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, art. 4 (1).

exigences ayant pour objet le type de technologies qui peut être utilisé[129]. Ces normes peuvent également viser l'évaluation de l'efficacité de ces services[130], sans oublier la collecte, la gestion et l'utilisation des données. Le législateur a néanmoins prévu un régime plus spécifique pour les « données ouvertes » qui peuvent être mises à la disposition du public, particulièrement en vue de l'élaboration de conditions relatives à des permis d'utilisation qui peuvent être attribués par un organisme du secteur public[131]. Si ces normes sont contraignantes pour les organismes du secteur public, elles échappent néanmoins aux exigences de la *Loi de 2006 sur la législation*[132], ce qui signifie qu'elles ne sont pas de nature réglementaire. Le directeur doit toutefois les divulguer sur un site Web du gouvernement de l'Ontario[133].

Le législateur ontarien a néanmoins prévu d'autres critères qui relèvent directement de la loi, en particulier pour les principes. Pour les organismes publics qui créent et utilisent des services numériques, ces principes insistent sur l'importance des utilisateurs, sur l'évaluation continue, sur la sécurité et la confidentialité des renseignements personnels, ainsi que sur l'utilisation « de plateformes technologiques évolutives, interopérables et réutilisables[134] ». En ce qui a trait aux données ouvertes, le législateur énumère des principes relatifs à la lisibilité technique, à la gratuité ou à la modération des frais, à l'exactitude ou à l'utilisation commerciale et non commerciale, pour ne donner que quelques exemples. Les organismes publics doivent offrir au directeur du numérique et des données un recensement et une description de leurs données et justifier, le

129 *Id.,* art. 4 (2).

130 Pour cette dimension, des mécanismes issus de la nouvelle gestion publique seront utilisés aux fins de mesure.

131 *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, par. 4 (3) d.

132 *Loi de 2006 sur la législation*, L.O. 2006, c.21.

133 Depuis quelques années, des normes relatives aux services numériques ont été élaborées : en ligne : < https://www.ontario.ca/fr/page/norme-des-services-numeriques >.

134 *Loi de 2019 pour des services simplifiés, accélérés et améliorés*, préc., note 1, art. 5 (1).

cas échéant, la non-divulgation au public[135]. Par commodité pour la suite de notre étude, nous considérerons ces données comme des « données fermées », même si le législateur n'emploie pas cette terminologie.

La loi ontarienne offre l'exemple d'un travail de pondération entre un cadre législatif de portée générale et l'utilisation subséquente de normes qui relèvent de la vaste famille des directives et des lignes directrices. Les autorités fédérales ont adopté une tout autre approche en créant dès 2007 la fonction de dirigeant principal de l'information du gouvernement du Canada et celle de dirigeant principal de l'information à l'échelle ministérielle, par la *Politique sur la gestion des technologies de l'information*[136]. Ces orientations ont été actualisées en 2020 par la *Politique sur les services et le numérique*[137] et par la directive sur le même sujet[138]. Comme ailleurs, les responsabilités qui incombent au dirigeant principal de l'information dépassent largement la simple protection des renseignements personnels, puisqu'il doit élaborer des « normes pangouvernementales » relatives à l'information et aux données, notamment pour l'utilisation des processus opérationnels de la technologie de l'information et pour la définition des exigences en matière de cybersécurité[139]. La *Politique sur les services et le numérique* vise également l'attribution de responsabilités plus spécifiques pour les administrateurs généraux des ministères et des organismes fédéraux, tout comme elle décrit le rôle de SPC dans l'offre de services numériques aux organismes fédéraux[140] et celui de Services publics et Approvisionnement Canada (SPAC), ministère du gouvernement du Canada. Par son contenu, la *Politique sur les services et le numérique* ressemble à certains égards à une loi, d'autant plus qu'elle offre en annexe 38 définitions qui sont d'un

135 *Id.,* art. 6 (1) a.

136 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 8, art. 6.2 et 6.4.

137 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services et le numérique*, préc., note 7.

138 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Directive sur les services et le numérique*, préc., note 7.

139 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 8, art. 4.3 et 4.4.

140 Services partagés Canada a été institué en 2012 sous forme de ministère : *Loi sur Services partagés Canada*, préc., note 116, art. 4.

grand intérêt pour ce processus de transition numérique[141]. En contrepartie, la *Directive sur les services et le numérique* a pour objet la désignation d'un dirigeant principal de l'information au sein des ministères et des organismes fédéraux, tels qu'ils sont définis par l'article 2 de la *Loi sur la gestion des finances publiques*[142]. Le contenu de cette directive est plus conforme aux finalités reconnues habituellement dans ce type de documents puisqu'elle offre, avec des annexes, des exemples d'utilisation acceptable ou inacceptable des dispositifs[143] et des réseaux.

En dépit de ces différences dans le choix des instruments, la transition numérique de l'administration publique répond à des objectifs similaires, tant au Québec et en Ontario qu'au niveau fédéral. En priorisant les enjeux relatifs à la répartition des responsabilités et des ressources au sein des organismes publics, les autorités ne semblent pas soucieuses d'inclure des dimensions variées concernant les droits des citoyens et des autres utilisateurs, comme si ce processus de transition était avant tout de nature administrative. La *Directive sur la prise de décision automatisée* constitue néanmoins une exception. Conçue de façon à « réduire les risques pour les Canadiens et les institutions fédérales », elle impose une évaluation de l'incidence algorithmique avant la production de tout système décisionnel automatisé, ainsi que des obligations en matière de transparence[144].

---

141 À titre comparatif, le SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 8, présente une politique qui ne contient que dix définitions.

142 La *Loi sur la gestion des finances publiques*, préc., note 60, art. 2, comporte, outre la liste des ministères fédéraux qui figure à l'annexe l, l'énumération des organismes fédéraux à l'annexe l.1.

143 Le SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services et le numérique,* préc., note 7, (définitions), précise que les « dispositifs » sont l'ensemble des outils électroniques, notamment tous les types d'ordinateurs, les blocs-notes et les tablettes électroniques, les téléphones cellulaires, les appareils périphériques (les imprimantes, les numériseurs, les outils qui servent à l'entreposage d'information, les lecteurs de CD et de DVD, les caméras Web), ainsi que tout autre type de matériel informatique.

144 *Directive sur la prise de décision automatisée*, préc., note 7, art. 6.1 et 6.2. Cette directive est commentée plus loin dans ce texte.

Par le dépôt du projet de loi nº 64 en juin 2020, afin d'introduire des modifications substantielles en matière de protection des renseignements personnels, le Québec s'oriente vers une rupture en matière de transition numérique[145]. La protection du public constitue désormais une priorité. Si ce projet de loi devait se traduire éventuellement par une nouvelle législation, le Québec se rapprocherait ainsi de ce qui a été fait par les Américains et les Européens.

II. Les enjeux liés à la protection des données

Afin de mieux comprendre la nature des changements contenus dans le projet de loi nº 64, nous estimons qu'un recul est indispensable, car il n'y a rien de comparable ailleurs au Canada. Du côté du droit européen, le RGPD offre un ensemble de droits et de garanties qui ne touchent pas précisément les administrations publiques. De façon générale, il a été conçu de façon à assurer, à titre de droit fondamental, la protection des personnes physiques à l'égard du traitement des données à caractère personnel[146]. La libre circulation des données à caractère personnel n'est pas interdite ni limitée par le RGPD. Certaines exceptions sont prévues, notamment pour le travail des autorités compétentes aux fins de prévention et de détection des infractions pénales. Parmi les définitions qui figurent à son article 4, celles qui concernent les « données à caractère personnel », le « traitement », le « profilage » et les « données biométriques » sont d'un grand intérêt pour évaluer des enjeux liés à la transition numérique des administrations publiques. Si le traitement de données sensibles est interdit sur le plan des principes, le RGPD prévoit tout de même plusieurs exceptions susceptibles de rejoindre les activités des administrations publiques, en particulier dans le domaine de la santé[147]. À la lumière de la pandémie de COVID-19, le traitement de données personnelles peut se révéler « nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique[148] ».

---

145 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi nº 64 (étude détaillée – 21 avril 2021), 1re sess., 42e légis. (Qc) (ci-après « projet de loi nº 64 »).

146 RGPD, préc., note 25, premier considérant.

147 *Id*., art. 9 (2).

148 *Id*., art. 9 (2) i.

À titre préliminaire, il n'est pas réaliste de proposer une étude détaillée et exhaustive du RGPD dans le but de tenir compte de la spécificité des administrations publiques. Malgré cette limite, la formulation de quelques dispositions montre que cette spécificité a été prise en considération. Ainsi pour le droit à l'effacement des données (« droit à l'oubli »), le RGPD contient des exceptions pour assurer le respect d'une obligation légale requise « pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » de données à caractère personnel[149]. Une ligne de partage se profile dans la mesure où l'intérêt public requiert des exceptions. En revanche, si l'État est engagé dans des activités de nature industrielle et commerciale par le recours à des entreprises publiques, cette spécificité devient moins évidente. L'interdiction du « profilage » par l'article 22 en est un exemple. Compte tenu de la définition qui en est donnée à l'article 5[150], des pratiques devenues courantes pourraient, *a priori* et en apparence, se voir interdites si, par hypothèse de travail, le RGPD était directement applicable en droit canadien. Par exemple, la Société des alcools du Québec offre à sa clientèle une carte de fidélité qui permet d'accumuler des points, mais qui facilite également, grâce à la pratique de l'historique des achats antérieurs, la présentation d'offres personnalisées. Ce type de profilage est très répandu pour les achats en ligne chez les géants du numérique, aussi appelés « GAFA[151] », qui peuvent offrir notamment des livres et des produits culturels susceptibles de répondre aux préférences personnelles des utilisateurs, selon les données induites par l'historique des acquisitions

149 *Id*., art. 17 (3) b.

150 *Id*., art. 5, où le « profilage » est ainsi défini :

> Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

151 GAFA est un acronyme qui permet de rassembler sous la même bannière quatre géants du WEB : Google, Apple, Facebook et Amazon. Cet acronyme sert également à englober d'autres grands acteurs du numérique : Microsoft, Yahoo, Linkedln et Twitter.

antérieures[152]. D'après la formulation de l'article 22 du RGPD, deux conditions doivent néanmoins être réunies : le traitement de l'information est exclusivement automatisé et produit des effets juridiques sur la personne visée[153]. Selon les exemples que nous avons énumérés, le simple profilage destiné à la promotion de produits échappe ainsi à l'application du RGPD. Une législation nationale pourrait cependant proscrire le profilage à des fins publicitaires, comme le montre le cas de l'Espagne qui a modifié en 2018 sa législation antérieure à la lumière du contenu général du RGPD[154].

En droit canadien, l'existence de législations propres aux secteurs public et privé en matière de protection de la vie privée et d'accès à l'information illustre le fait que le législateur a tenu compte de la spécificité des administrations publiques[155]. En revanche, de manière plus générale, l'évolution du droit administratif traduit une ligne de partage inégale et poreuse entre l'application du régime général de droit commun par rapport à l'utilisation de règles précises issues du droit public. Ces dernières ont néanmoins la priorité dans la détermination du droit applicable. Dans un

---

152 Ce profilage repose sur l'analyse du comportement de l'utilisateur, notamment par l'usage de cookies : Sarit MIZRAHI, *The Legal Implications of Internet Marketing: Exploiting the Digital Marketplace within the Boundaries of the Law*, Montréal, Éditions Yvon Blais, 2015, p. 11.

153 Anne DANIS-FATÔME, « Décisions automatisées et profilage », dans Alexandra BENSAMOUN et Brunessen BERTRAND (dir.), *Le règlement général sur la protection des données. Aspects institutionnels et matériels*, Paris, Éditions Mare et Martin, 2020, p. 198.

154 *Ley Organica 3/2018, de 5 de diciembre, de Proteccion de Datos Personales y garantia de los derechos digitales* (Loi organique de protection des données à caractère personnel et des droits numériques), BOE-A-2018-16673, art. 23 (Sistemas de exclusion publicitaria), en ligne : < https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf >.

155 En droit fédéral, la Loi sur l'accès à l'information, L.R.C. 1985, c. A-1, et la Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21, visent l'administration fédérale, par opposition à la première partie de la *Loi sur la protection des renseignements personnels et les documents électroniques*, préc., note 9, qui vise le secteur privé. Le Québec offre la même ligne de partage avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, par opposition à la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1.

arrêt unanime qui remonte à 2004, la Cour suprême du Canada a tenu à rappeler, à propos de la formulation de l'article 1376 du *Code civil du Québec*, que « la prudence du législateur reflète la spécificité de l'administration publique, ainsi que la diversité et la complexité des tâches qui lui sont dévolues[156] ». En dépit du fait que des organismes publics peuvent se trouver dans une situation comparable ou analogue à celle d'autres organisations pour le recours à l'infonuagique ou l'utilisation des algorithmes, le cadre juridique peut différer substantiellement en raison des dimensions de droit administratif et de droit public général.

A) La confidentialité des renseignements personnels

L'analyse de ces enjeux reste tributaire du contenu des lois de transition numérique ainsi que des lois relatives à la protection de la vie privée et des données personnelles. La pondération de ces deux types de législation peut être déterminante pour mettre en relief la qualité du cadre juridique offert à la population ou, à l'inverse, montrer des lacunes qui ne sont que trop évidentes. Ce dispositif suppose l'harmonisation d'une ou, le cas échéant, de plusieurs lois relatives à la transition numérique avec le contenu des lois sur la protection de la vie privée qui remontent dans l'ensemble, à quelques exceptions près, aux années 70 et 80.

À titre d'exemple, l'approche américaine montre que l'*E-Government Act* de 2002 a été rédigée de façon à raffermir et à inclure les dispositions de la *Privacy Act* de 1974[157], même si certaines parties de la loi de 2002 visent la protection de la confidentialité sans lien explicite avec la loi de 1974[158]. L'approche retenue par le Québec ne montre pas ce type de

156 Comme il est question d'une poursuite en responsabilité civile dirigée contre un organisme public, la « Cour reconnaît que des principes généraux ou des règles de droit public spécifiques peuvent soit faire obstacle à toute application du régime général de responsabilité civile, soit en modifier substantiellement les règles de fonctionnement » : *Finney* c. *Barreau du Québec*, 2004 CSC 36, par. 27.

157 À titre d'exemple, dans l'élaboration des politiques relatives à la confidentialité qui sont consultables sur leur site Web, les agences fédérales doivent impérativement tenir compte des exigences de la *Privacy Act*, préc., note 112.

158 Dans cette perspective, le titre V a pour objet la protection de l'information de nature confidentielle récoltée à des fins statistiques : *E-Government Act of 2002*,

lien, bien que cette situation puisse évoluer. Dans la situation actuelle, avant le dépôt du projet de loi nº 64[159], les autorités ou les organismes chargés de la transition numérique ont la responsabilité générale de veiller à la confidentialité des données, parfois sans trop de précisions. Infrastructures technologiques Québec doit ainsi « veiller au respect des normes propres à assurer l'intégrité, la confidentialité et l'accessibilité de l'information des organismes publics qu'il détient notamment par la mise en place de mesures de sécurité[160] ». Dans la loi de 2019, les renseignements personnels servant à la réalisation d'un projet en ressources informationnelles d'intérêt gouvernemental ne peuvent être utilisés que dans ce but par l'organisme public, avec des mesures de sécurité propres à assurer leur protection[161]. Le gouvernement peut également édicter des règles particulières de protection des renseignements personnels s'il « existe un degré élevé d'attente raisonnable en matière de vie privée », sous réserve des exigences déjà prévues dans une loi ou un règlement[162]. Dans la loi de 2011, c'est le Conseil du trésor qui peut, le cas échéant, « prendre une directive » afin de « prévoir des règles pour assurer la sécurité des ressources informationnelles, y compris la protection des renseignements personnels et des autres renseignements qui ont un caractère confidentiel »[163]. En contrepartie, selon la formulation retenue par le législateur, le rôle du dirigeant principal de l'information et des dirigeants de l'information serait davantage orienté vers l'élaboration d'une « vision globale[164] » aux fins de « transformation organisationnelle[165] » pour chaque organisme public tel

préc., note 103 (« Confidential Information Protection and Statistical Efficiency »).

159 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 145.

160 *Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec*, préc., note 3, art. 4 (5) de la loi édictée par l'article 2 de la loi omnibus.

161 *Loi favorisant la transition numérique de l'administration publique*, préc., note 2, art. 4.

162 *Id*., art. 6.

163 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 20 al. 2 (1).

164 *Id*., art. 7 (0.1).

165 *Id*., art. 10.1 al. 1 (2).

qu'il est défini par l'article 2 de la loi de 2011. Leur rôle respectif est en fait précisé dans la *Directive sur la sécurité de l'information gouvernementale* adoptée en 2014[166]. Outre le dépôt de rapports annuels ou bisannuels auprès du Conseil du trésor, le dirigeant principal de l'information doit proposer un cadre gouvernemental de gestion de la sécurité, ainsi qu'un cadre de gestion des risques et une approche stratégique triennale[167]. De plus, il est responsable de l'application des politiques et des directives qui découlent de la mise en œuvre de la loi[168].

L'esprit général de ces réformes montre la prépondérance des impératifs de sécurité, de ressources organisationnelles, de partage des responsabilités entre unités administratives, de même que l'importance de l'efficience et de l'efficacité en vue de l'amélioration et de l'optimisation des coûts d'exploitation. La transition numérique restant ainsi orientée vers le fonctionnement des administrations publiques, ce qui pouvait relever de l'évidence montrait, en réalité, un déséquilibre au profit des impératifs de gestion. La simple comparaison avec l'*E-government Act* et le RGPD permet de recentrer l'analyse sur les droits des usagers (citoyens,

166 CONSEIL DU TRÉSOR DU QUÉBEC, *Directive sur la sécurité de l'information gouvernementale*, 2014, en ligne : < https://www.tresor.gouv.qc.ca/ressources-informationnelles/securite-de-linformation/directive-sur-la-securite-de-linformation-gouvernementale/ >.

167 *Id*., art. 6. Dès 2014, les instruments prévus par cette directive étaient consultables sur le Web : CONSEIL DU TRÉSOR DU QUÉBEC, *Cadre gouvernemental de gestion*, 2014, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_securite_information.pdf >; CONSEIL DU TRÉSOR DU QUÉBEC, *Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information*, 2014, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_risques_incidents.pdf >; CONSEIL DU TRÉSOR DU QUÉBEC, *Approche stratégique gouvernementale en sécurité de l'information 2014-2017*, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/approche_strategique_gouvernementale.pdf >.
Compte tenu de la création d'Infrastructures technologiques Québec et de l'abolition du Centre de services partagés du Québec en 2020, ces instruments seront, selon toute vraisemblance, modifiés.

168 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 7 (1).

organisations et entreprises). Outre la question du consentement requis sur la page Web des organismes fédéraux afin d'obtenir des renseignements de la part des individus, la loi américaine soulève explicitement, par le contenu exigé pour la réalisation des études d'impact, les enjeux liés à la nature de l'information recueillie et l'utilisation qui en est faite[169]. En réalité, les agences doivent, afin de clarifier ces enjeux, élaborer des politiques de confidentialité (*privacy policies*) et les inclure dans leur site Web[170].

Grâce au dépôt du projet de loi nº 64, la législation québécoise sera relativement similaire, sous réserve de quelques nuances, pour l'affichage électronique des organismes publics. Avant d'en mesurer la portée, nous croyons utile de revoir le contenu du droit actuel (à jour en 2020; 2020-2021). Les exigences législatives en matière de collecte de renseignements personnels offrent quelques balises. Hormis les renseignements personnels ayant un caractère public (généralement les nom et adresse des titulaires de permis et de ceux qui bénéficient d'un avantage économique conféré par un organisme public) qui peuvent être divulgués[171], l'information ainsi obtenue demeure confidentielle, sauf si la personne visée consent à sa divulgation[172], et sous réserve des exceptions prévues par la loi[173]. Pour l'utilisation et la conservation des renseignements plus sensibles[174], la législation québécoise reste contraignante, car « un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli[175] »;

169 *E-Government Act of 2002*, préc., note 103, art. 208.

170 Sous la rubrique « Privacy Policies on Websites », l'article 208 oblige les agences fédérales à tenir compte des exigences de l'article 552a de la *Privacy Act of 1978*, préc., note 112 *:* « What information is to be collected, why.., with whom the information will be shared, how the information will be secured. »

171 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, art. 55 et 57; un organisme public peut néanmoins refuser l'accès à ces renseignements, ou en restreindre l'accès, s'il est convaincu, pour des motifs raisonnables, qu'ils seront utilisés à des fins illégitimes (art. 55 al. 2).

172 *Id*., art. 53 (1).

173 *Id.,* art. 59 et 59.1.

174 À titre d'exemple : PORTAIL SANTÉ QUÉBEC, en ligne : < http://sante.gouv.qc.ca >.

175 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, art. 65.1

on compte néanmoins des exceptions, notamment lorsque la communication est nécessaire à l'application d'une loi, d'une convention collective ou d'un texte contraignant relatif à des conditions de travail et pour l'exécution d'un contrat de service[176]. L'harmonisation de ces exigences avec les nouveaux objectifs de la loi de 2019 sur la transition numérique n'était pas chose facile. En vertu de l'article 3 de cette loi, un organisme public désigné par le gouvernement peut transmettre « à toute personne ou à tout organisme les renseignements personnels qu'il détient dès lors que cette utilisation ou cette communication est nécessaire à la réalisation d'un projet en ressources informationnelles d'intérêt gouvernemental[177] ». Les modalités d'application peuvent être précisées par décret dans un contexte où cet article peut être appliqué malgré toute disposition inconciliable d'une loi. Même si la Commission d'accès peut donner son avis sur ce type de projet (art. 8), des renseignements personnels peuvent ainsi servir à des finalités autres que celles qui ont été prévues initialement pour un seul organisme, et ce, afin de passer à l'étape subséquente du partage de données entre plusieurs organismes. Dans la *Stratégie de transformation numérique*, le Québec étudie l'implantation d'un système d'accès unique (*Accès UniQc*)[178]. Dans cette stratégie, les autorités québécoises avaient manifesté leur volonté de modifier la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* afin de permettre cet accès unique[179].

Les modifications offertes par le projet de loi n^{o} 64 priorisent le consentement et la transparence. Le chapitre 3 (« Protection des renseignements personnels ») de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* sera modifié de façon à assurer un consentement libre, manifeste, éclairé et à des

176 *Id*., art. 65.1-67.2.

177 *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2, art. 3 al. 1.

178 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, préc., note 12, p. 15 et 16.

179 *Id*., p. 20 et 21.

fins spécifiques en matière de divulgation de renseignements personnels[180]. L'influence de l'*E-Government Act* de 2002[181] est ici manifeste avec une nouvelle série de dispositions relatives à la collecte et à l'utilisation des renseignements personnels. Les organismes publics auront la responsabilité de publier sur leur site Web des règles de gouvernance concernant les renseignements personnels et une « politique de confidentialité rédigée en termes simples et clairs[182] ». En contrepartie, l'influence européenne est visible avec une nouvelle disposition qui porte sur le profilage. C'est une grande innovation : les organismes publics auront désormais l'obligation d'informer les personnes visées qu'ils utiliseront des technologies comprenant des fonctions susceptibles de les identifier, de les localiser ou d'effectuer du profilage, ce dernier étant expressément défini par le projet de loi nº 64[183]. Cette approche correspond à celle du RGPD dans la mesure où le profilage aux fins d'un processus décisionnel est autorisé si le consentement explicite de la personne visée a été donné[184]. La formulation de la loi québécoise se révèle plus générale, car elle ne vise pas de façon précise un processus décisionnel.

Dans le projet de loi nº 64, les organismes publics auront également l'obligation de procéder à des évaluations des facteurs liés à la vie privée pour tout système électronique de services impliquant le traitement de renseignements personnels. Sur ce point, la *Loi d'accès aux documents des*

180 Projet de loi nº 64, préc., note 145, art. 9 (ajout de l'article 53.1 à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

181 *E-Government Act of 2002*, préc., note 103.

182 Projet de loi, nº 64, préc., note 145, art. 14 (ajout des articles 63.3 et suivants à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

183 « Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse de rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne » : projet de loi nº 64, préc., note 145, art. 18 (ajout de l'article 65.0.1 à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

184 RGPD, préc., note 25, art. 22.

organismes publics et sur la protection des renseignements personnels sera modifiée de façon à mieux encadrer l'utilisation des renseignements personnels concernant la divulgation[185]. À l'heure actuelle, l'anonymisation de données sensibles est permise aux fins d'étude, de recherche ou de production de statistique. Des conditions précises sont énumérées pour la divulgation de renseignements personnels sans le consentement des personnes visées, notamment pour la recherche ou la production de statistiques dans la perspective du respect d'un protocole de recherche[186]. Une disposition novatrice est prévue pour la communication des renseignements personnels à l'extérieur du Québec. Les organismes publics devront dès lors tenir compte du degré d'équivalence du régime juridique applicable dans l'État où le renseignement serait communiqué par rapport aux principes de protection applicables au Québec[187]. Les autorités n'ont pas renoncé au partage de renseignements personnels entre plusieurs organismes. Le gouvernement peut ainsi désigner, après consultation de la Commission d'accès à l'information, un ou plusieurs organismes afin d'exercer la fonction de « gestionnaire de renseignements personnels » suivant un cadre général déterminé par la loi[188]. Cependant, cette fonction ne doit pas être confondue avec celle de dirigeant principal de l'information qui découle de la loi de 2011[189].

185 L'actuel article 65.1 sera bonifié pour prévoir le consentement explicite des personnes visées : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24.

186 La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, sera modifiée par l'ajout des articles 67.2.1 à 67.2.3 qui visent expressément la recherche et la production de statistiques.

187 Projet de loi nº 64, préc., note 145, art. 27 (remplacement de l'article 70.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

188 La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, est modifiée par l'ajout des articles 70.3 à 70.7.

189 *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 6 et 7.

Ce nouveau cadre juridique, encore en gestation, pourrait être pris en considération dans le contexte des moyens envisagés afin de remédier à la propagation de la COVID-19. Bien avant que les autorités québécoises instaurent en septembre 2020 l'application Alerte COVID, le projet d'application StopCovid était en voie d'expérimentation du côté européen, comme le montre l'exemple de la France[190]. Interpellée sur ce projet, la Commission nationale de l'informatique et des libertés (CNIL) avait rendu un avis le 24 avril 2020[191]. Il est utile de rappeler que StopCovid est une application française de suivi de contacts dont la seule utilité consiste à informer les personnes qui l'ont installée sur leur téléphone intelligent qu'elles se trouvent à proximité d'une personne ayant le même dispositif et qui aurait reçu un diagnostic de COVID-19. Ce n'est donc pas une application de géolocalisation qui permettrait de repérer et de suivre en temps réel les personnes ayant obtenu un résultat positif à la COVID-19. Dans le contexte du droit européen, l'application StopCovid implique toutefois un traitement de données à caractère personnel à la lumière des dispositions du RGPD[192]. À première vue, il serait possible d'argumenter que les données ainsi collectées ne relèvent pas du contrôle d'une administration publique. En dépit des apparences, ce scénario ne peut être éludé, car l'application StopCovid est une construction à deux étages qui implique l'utilisation d'une application mobile installée sur le téléphone intelligent (*smartphone*), ainsi qu'un serveur central aux fins de compilation de données pseudonomysées. La reconnaissance de la personne infectée par ce serveur central reste néanmoins requise afin de l'informer. Dans son avis, la CNIL a tracé des lignes rouges, notamment pour que l'utilisation de l'application StopCovid reste volontaire, et ne puisse pas devenir un outil de surveillance[193].

---

190 *Supra*, note 33.

191 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »*, en ligne : < https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf >.

192 Les « données à caractère personnel » font l'objet d'une définition à l'article 4 du RGPD, préc., note 25.

193 Pour un commentaire sur cet avis, voir Olivia TAMBOU, « Que retenir de l'avis de la CNIL sur le projet d'application mobile ' StopCovid ' », *Le Club des juristes*,

Compte tenu des enjeux sanitaires, l'intervention d'une autorité publique est requise afin d'autoriser l'implantation de ce type d'application. Au Québec, cette autorité est en principe le directeur national de la santé publique, et le ministre de la Santé et des Services sociaux[194], sous réserve des positions que peuvent exprimer le premier ministre et l'Assemblée nationale. La nécessité d'un fondement juridique explicite et précis ne peut être éludée[195]. Au printemps 2020, un projet à l'étude avait pour objet de confier aux universités l'hébergement des serveurs de gestion de l'application StopCovid afin d'éviter le partage d'information avec les autorités gouvernementales[196]. Comme il était question d'un projet en ressource informationnelle, les universités pouvaient agir sur le fondement de lois préexistantes[197].

La Commission des institutions de l'Assemblée nationale avait recommandé, en août 2020, d'éviter d'utiliser ce type d'application de traçage dans le cas des personnes infectées par la COVID-19[198]. Pour les dimensions juridiques, la Commission des institutions aurait bénéficié d'un autre éclairage si le contenu du projet de loi nº 64 avait franchi toutes les étapes en vue de devenir la législation applicable. Concernant l'utilisation de technologies de localisation et de profilage, ce projet de loi prévoit que les personnes visées doivent en être informées, notamment afin de les prévenir « des moyens offerts, le cas échéant, pour désactiver les fonctions

Blog du coronavirus, 29 avril 2020, en ligne : < https://www.leclubdesjuristes.com/blog-du-coronavirus/que-dit-le-droit/que-retenir-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid/ >.

194 *Loi sur la santé publique*, RLRQ, c. S-2.2, art. 2 et 34.

195 Plusieurs dispositions de la *Loi sur la santé publique*, préc., note 194, confèrent de vastes pouvoirs aux autorités de la santé, notamment les articles 55 et 56.

196 Tristan PÉLOQUIN, « Application de traçage : le projet québécois prend forme », *La Presse*, 20 mai 2020, en ligne : < https://www.lapresse.ca/covid-19/2020-05-10/application-de-tracage-le-projet-quebecois-prend-forme >.

197 *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2, art. 2 et 3; *Loi sur la gouvernance et la gestion des ressources informationnelles*, préc., note 4, art. 2 (organismes publics).

198 *Supra*, note 36.

permettant d'identifier, de localiser ou d'effectuer un profilage[199] ». En l'absence de loi spécifique pour autoriser ce type de moyen, le Québec n'en a pas moins pris la décision d'utiliser l'application Alerte COVID élaborée par les autorités fédérales[200]. La prudence demeure de rigueur, car cette application ne repose pas sur des données nominatives et de la géolocalisation[201]. Cette dernière reste interdite, à moins que la loi ne le prévoit expressément, en particulier dans le domaine de la santé et de la sécurité[202].

B) Le recours à l'infonuagique publique

Pour réaliser le partage d'information entre l'ensemble des organismes publics, le recours à l'infonuagique est en plein essor dans les administrations publiques. Si le Québec a manifesté en 2019 l'intention d'amorcer un virage vers l'infonuagique[203], les autorités fédérales, quant à elles, avaient élaboré en 2016 la *Stratégie d'adoption de l'informatique en nuage du gouvernement*[204]. En fait, dès 2007, l'utilisation des services d'informatique en nuage avait été priorisée[205]. Les modèles de services

199 Projet de loi nº 64, préc., note 145, art. 18 (ajout de l'article 65.0.1 à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

200 *Supra*, note 37.

201 GOUVERNEMENT DU CANADA, « Comment l'appli Alerte Covid fonctionne », 2020, en ligne : < https://www.canada.ca/fr/sante-publique/services/video/alerte-covid.html >.

202 « À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve » : *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 43 al. 2.

203 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, préc., note 12, nº 12 (« Lancer le programme d'adoption de l'infonuagique »).

204 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018*, Ottawa, 2018, en ligne : < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html >

205 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 8, art. 6.2.6.

offerts en infonuagique peuvent varier substantiellement selon la mise à disposition d'un réseau qui permette d'éliminer l'utilisation de logiciels dans des ordinateurs locaux par opposition à un modèle plus répandu, où les utilisateurs achètent de l'espace de stockage dans le nuage en fonction de leur consommation[206]. Ce « nuage public » se trouve à l'extérieur de l'organisation et offre la possibilité de partager la même infrastructure de logiciels avec d'autres utilisateurs ou organismes[207]. Les organismes publics peuvent ainsi transmettre des données à des sociétés privées, à des organismes sans but lucratif et à des particuliers. En contrepartie, le nuage privé offre au gouvernement du Canada la possibilité d'être le seul utilisateur. En 2007, toutes les données électroniques sous contrôle des autorités fédérales (avec divers types de classement, notamment « Protégé B », « Protégé C » ou classifiées selon le niveau de secret[208]) devaient être stockées dans une installation informatique approuvée par le gouvernement du Canada et située à l'intérieur des frontières géographiques du pays (ou dans une mission diplomatique ou consulaire canadienne à l'étranger)[209]. Si, d'un point de vue factuel et matériel, les données se trouvent au Canada, elles sont assujetties aux lois canadiennes sur la protection des renseignements personnels.

Dans un contexte où le nuage public devient « l'option privilégiée pour la prestation de services de la [technologie de l'information][210] », le gouvernement du Canada a diffusé un livre blanc intitulé *Souveraineté des*

206 CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, « Infonuagique : les types », 10 janvier 2019, en ligne : < https://cyber.gc.ca/fr/infonuagique-les-types >.

207 W. Kuan HON et Christopher MILLARD, « Cloud Technologies and Services », dans Christopher MILLARD (dir.), *Cloud Computing Law*, New York, Oxford University Press, 2013, p. 4 (catégories de services).

208 Les cotes utilisées par les autorités fédérales sont « Protégé A, B et C, ainsi que Confidentiel, Secret et Très secret » : TRAVAUX PUBLICS ET SERVICES GOUVERNEMENTAUX CANADA, *Niveaux de sécurité s'appliquant aux renseignements et aux biens de nature délicate du gouvernement*, en ligne :< www.tpsgc-pwgsc.gc.ca >.

209 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 8, art. 6.2.7.

210 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 204 (« Introduction »).

données et nuage public en 2018[211]. Dans ce document, le Conseil du Trésor évalue les risques que pose le recours à des fournisseurs de services d'informatique en nuage (FSIN) qui sont des organisations à grande échelle dont les activités permettent une diffusion mondiale. *A priori*, cette déterritorialisation dans le nuage ne permettrait pas au Canada de conserver la pleine souveraineté de ses propres données puisqu'un FSIN peut être assujetti à la législation d'un autre pays avec des contraintes de divulgation. Afin de remédier à ce problème, le gouvernement du Canada a publié en 2017 l'*Orientation relative à la résidence des données électroniques*[212]. Ce texte oblige les ministères et les organismes fédéraux à chiffrer toutes les données électroniques du gouvernement du Canada lorsqu'elles sont transmises hors des zones de travail et des zones de sécurité du pays[213]. Selon le livre blanc de 2018, le risque principal pour la souveraineté des données serait du côté américain compte tenu de la portée de la *Foreign Intelligence Surveillance Act* de 1978 (avec modifications subséquentes) qui permet aux autorités américaines, notamment la Central Intelligence Agency (CIA), de faire de la surveillance électronique afin de collecter des informations (*foreign intelligence information*) en provenance de puissances étrangères suspectées d'espionnage ou de terrorisme[214]. En réalité, la plus grande menace découle de l'entrée en vigueur de la *CLOUD*

211 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Livre blanc du Gouvernement du Canada : Souveraineté des données et nuage public*, Ottawa, 2018, en ligne : < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/gc-livre-blanc-souverainete-donnees-nuage-public.html > (ci-après « livre blanc »).

212 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Orientation relative à la résidence des données électroniques*, Ottawa, 2017, en ligne : < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-relative-residence-donnees-electroniques.html >

213 *Id*. : « Les données électroniques des catégories ' Protégé B ' et ' Protégé C ' sont des données qui, lorsqu'elles sont compromises, pourraient entraîner un préjudice grave ou extrêmement grave à une personne, à une organisation ou au gouvernement. »

214 *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95-511, 92 Stat. 1783 (1978); 50 U.S.C. § 36.

Act le 28 mars 2018[215], car cette loi permet dorénavant aux autorités américaines, en particulier au Federal Bureau of Investigation (FBI), de contraindre, par mandat ou assignation, les FSIN à fournir les données demandées qui sont entreposées dans le nuage, peu importe que les serveurs soient situés aux États-Unis ou ailleurs.

Devant ces atteintes potentielles à la souveraineté numérique du Canada[216], le livre blanc recommande de suivre l'exemple d'autres pays en limitant les catégories de données qui peuvent être stockées dans le nuage[217]. Sa porosité est un fait connu[218]. Cette recommandation ne semble pas être suivie puisque des organismes fédéraux, notamment Statistique Canada, prévoient le transfert de banques de données dans le nuage informatique. Le procédé du chiffrement peut constituer une solution de rechange en protégeant les renseignements personnels par le moyen d'un algorithme cryptographique qui rend l'information hors de portée de ceux qui n'ont pas la clé de déchiffrement. Dans cette recherche de solutions, les autorités fédérales sont aux prises avec le vieillissement de l'infrastructure de la technologie de l'information. Elles sont ainsi conduites à évaluer plusieurs possibilités en matière de cybersécurité. Dans les « réponses du gouvernement concernant la souveraineté des données » présentées à la fin du livre blanc, certaines façons de faire, comme l'utilisation de clauses contractuelles afin d'obliger les FSIN à maintenir la confidentialité ou

---

215 La *Clarifying Lawful Overseas Use of Data (CLOUD) Act,* a été insérée dans une loi omnibus, la *Consolidated Appropriations Act, 2018*, *Division V – Cloud Act*, Pub. L. No. 115-141, 132 Stat. 348. Auparavant, avant qu'elle soit modifiée, la *Stored Communications Act*, 18 U.S.C. § 121 (1986), prévoyait une demande d'entraide judiciaire internationale fondée sur des traités bilatéraux afin d'obtenir des documents stockés à l'étranger par une entreprise américaine. Cette solution est offerte par la *Convention de Budapest de 2001 sur la cybercriminalité*, STE nº 185, chap. III (« Coopération internationale »).

216 Dans une perspective comparée, voir Pauline TÜRK et Christian VALLAR (dir.), *La souveraineté numérique. Le concept, les enjeux*, Paris, Éditions Mare et Martin, 2017.

217 Livre blanc, préc., note 211 (« Souveraineté des données et mesures d'atténuation »).

218 Peter K. YU, « Towards the Seamless Global Distribution of Cloud Content », dans Anne S.Y. CHEUNG et Rolf H. WEBER, *Privacy and Legal Issues in Cloud Computing*, Cheltenham (UK), Edward Elgar, 2015, p. 180.

encore l'obtention par ces derniers de certificats de sécurité reconnus à l'échelle internationale du type ISO 27001, ne peuvent pas atténuer la portée de lois qui ne relèvent plus de la souveraineté du Canada. Parmi les possibilités qui semblent plus satisfaisantes, le chiffrement des données ou leur masquage par l'anonymisation paraissent déjà davantage réalistes. L'option qui consiste à limiter le type de données qui peuvent être entreposées dans le nuage public s'avère la plus sécuritaire[219]. Le stockage des données en territoire canadien pourrait aussi être une solution, à l'image de ce qui a été fait en Colombie-Britannique en 2012. Cette réponse au problème, fondée sur la « résidence » des données, découle d'une volonté d'harmonisation avec la législation relative à la vie privée de la Colombie-Britannique[220]. Si les serveurs sont situés en territoire canadien, l'application de la législation canadienne et québécoise devient plus plausible. Ainsi, l'article 26 de la loi relative au cadre juridique des technologies de l'information oblige le prestataire de services responsable de la conservation de documents technologiques à protéger la confidentialité et à interdire l'accès à des tiers non autorisés[221]. Cette garantie est importante pour les ordres professionnels qui imposent des obligations de confidentialité à leurs membres. Mais comme les dispositions du projet de loi C-11 sont favorables à la circulation et à la divulgation de renseignements personnels à l'insu et sans le consentement de la personne intéressée[222], un travail de pondération sera nécessaire.

Comme le montre l'exemple de Statistique Canada, la conjonction qui résulte du très grand volume de données accumulées au fil des décennies et de la désuétude relative des technologies de l'information au sein des

219 Pour le Canada, cette option peut inclure les données de niveau « Protégé B » inclusivement.

220 Le Bureau du commissaire à l'information et à la protection de la vie privée a publié en janvier 2012 des lignes directrices sur l'informatique en nuage pour les organismes publics : OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONNER FOR B.C., *Cloud Computing Guidelines for Public Bodies*, 2012, en ligne : < https://bcerac.ca/wp-content/uploads/2018/05/Cloud-Computing-Guidelines-2012.pdf >.

221 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 26 al. 2.

222 *Projet de loi C-11*, préc., note 11, arts. 43 à 48.

administrations publiques afin de les conserver rendrait inéluctable le recours grandissant à l'infonuagique publique. Une telle pression surgit à un moment où la législation relative à la protection de la vie privée avait été conçue suivant d'autres prémisses. Ainsi, la *Loi* fédérale *sur la protection des renseignements personnels* précise que « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités[223] ». À défaut du consentement de l'individu visé, les renseignements personnels relevant d'une institution fédérale ne peuvent servir « qu'aux fins auxquelles ils ont été recueillis », de même « que pour les usages qui sont compatibles avec ces fins »[224]. Si cette formulation ne fait pas obstacle, *a priori*, à l'infonuagique pour les besoins d'une institution fédérale, en revanche, elle ne permet pas le partage des renseignements personnels avec d'autres organismes ou ministères fédéraux (à moins de programmes communs), et encore moins avec des tiers externes. Cependant, la loi fédérale a le mérite d'offrir une définition précise de ce qu'il faut inclure dans les renseignements personnels[225]. En l'absence de mesures appropriées de sécurité, le recours à l'infonuagique publique présente des risques considérables qui ont été recensés et analysés dans le livre blanc de 2018[226]. Dans son rapport annuel déposé en décembre 2019, le Commissaire à la vie privée constate que la législation fédérale a pour objet la protection des renseignements personnels, sans reconnaître pour autant un « véritable » droit à la vie privée[227]. Même si la Cour suprême a posé des balises en matière de vie privée, notamment dans l'affaire *R.* c. *Spencer* en 2014[228], le

223 *Loi sur la protection des renseignements personnels*, préc., note 155, art. 4.

224 *Id*., art. 7 a).

225 *Id*., art. 3 (définitions).

226 Livre blanc, préc., note 211.

227 « Quoique ces deux lois [*Loi sur la protection des renseignements personnels / Loi sur la protection des renseignements personnels et les documents électroniques*] garantissent le droit d'accès des individus aux renseignements personnels qui les concernent […], aucune ne reconnaît officiellement le droit à la vie privée comme un droit en soi » : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Réforme des lois sur la vie privée, Rapport annuel 2018-2019*, Gatineau, 2019, p. 11.

228 Dans cet arrêt relatif à la vie privée des internautes, notamment en matière de fouille à l'égard d'un ordinateur utilisé à domicile, la Cour suprême, unanime, a

Commissaire rappelle, à juste titre, que la législation actuelle est trop étroite, et qu'elle devrait être adaptée à l'ère numérique. Il a critiqué la *Charte canadienne du numérique*, jugée peu efficace afin de garantir le respect de la vie privée des Canadiens[229]. Aux fins de notre étude, nous devons reconnaître que les principes énoncés dans cette charte visent des dimensions plus vastes que la transition numérique des administrations publiques[230], ce que confirme le dépôt du projet de loi C-11 qui propose un premier cadre juridique pour la protection des renseignements personnels en matière de commerce électronique[231]. Il n'en revêt pas moins un réel intérêt pour la question de l'infonuagique puisque les « fournisseurs de services d'informatique en nuages » (FSNI) répondent au critère de « l'activité commerciale ». Même s'il s'agit « d'activités d'affaires », ces fournisseurs n'en restent pas moins des opérateurs qui diffèrent de ceux principalement visés par ce projet de loi, lesquels correspondent à des serveurs auxquels le grand public a accès. En dépit de l'objectif général de protection, C-11 présente de nombreuses exceptions afin de faciliter l'accès à des renseignements personnels sans le consentement des intéressés, ou à leur insu. Compte tenu de la portée extraterritoriale de la loi proposée[232], ce projet de loi offre un cadre juridique afin de permettre à des institutions gouvernementales, au premier rang desquels figurent les services de sécurité et les différents corps policiers, d'obtenir des renseignements stockés en mode infonuagique[233]. Bien que ce ne soit pas l'objectif général de ce projet de loi, il offre ainsi des possibilités comparables à celles offertes par le CLOUD Act[234] dans un contexte où l'extraterritorialité des

reconnu trois principes, soit la confidentialité, le contrôle de l'information et l'anonymat : *R.* c. *Spencer*, 2014 CSC 43.

229 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 227, p. 5.

230 À titre d'exemple, le 9e principe vise le contenu des plateformes numériques afin d'éviter qu'elles diffusent des discours haineux ou du contenu criminel, ainsi que la promotion de l'extrémisme violent : *Charte canadienne du numérique*, préc., note 10.

231 *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, projet de loi C-11, préc., note 11.

232 *Id.*, par. 6(2).

233 *Id.*, art. 43 et suiv. (Communication à une institution gouvernementale).

234 *CLOUD Act*, préc., note 215.

interventions législatives et réglementaires devient de plus en plus la règle[235].

C) L'utilisation des données biométriques

Il est important de clarifier le statut des données qui découlent de renseignements biométriques[236]. Si les agents conversationnels (*chatbots*) peuvent analyser et enregistrer des données qui découlent de l'expression verbale d'un utilisateur[237], avec des perspectives de transfert vers l'infonuagique[238], le mécanisme de la reconnaissance faciale est désormais très répandu pour le déverrouillage des téléphones intelligents. Pour le moment, ils ne semblent pas, sauf une exception notable qui vise les

235 « ..on both sides of the Atlantic and beyond, jurisdictions increasingly endeavor to apply their legislation extraterritorially »; Federico FABBRINI, Edoardo CELESTE et John QUINN, (dir.), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford / New York, Hart, 2021, p. 2.

236 La Commission d'accès à l'information du Québec rappelle que « les systèmes biométriques sont généralement classés par l'industrie dans deux grandes catégories : la biométrie morphologique ou physiologique et la biométrie comportementale ». Si la première catégorie regroupe les empreintes digitales, la forme de la main, la forme du visage, la rétine et l'iris de l'œil, la seconde a notamment pour objet le décodage de la voix, la signature, la démarche : COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec*, Québec, 2016, en ligne : < https://www.cai.gouv.qc.ca/biometrie/ >. La reconnaissance par la démarche corporelle est déjà utilisée en Chine : « Chine : une intelligence artificielle reconnaît les gens à leur démarche», *20 minutes*, 8 novembre 2018, en ligne : < https://www.20minutes.fr/monde/2368119-20181108-chine-intelligence-artificielle-reconnait-gens-demarche >. Pour en savoir davantage sur ces enjeux, voir Stan Z. LI et Anil K. JAIN (dir.), *Encyclopedia of Biometrics*, 2e éd., Boston, Springer, 2015.

237 Alain BENSOUSSAN et Jérémy BENSOUSSAN, *IA, robots et droit*, Bruxelles, Bruylant, 2019 , titre III, chap. 4 « Les chabots », p. 227 et suiv.

238 Sarit K. MIZRAHI, « A Whole New Meaning to Having our Head in the Clouds : Voice Recognition Technology, the Transmission of our Oral Communications to the Cloud and the Ability of Canadian Law to Protect Us from the Dangers it Presents », (2017) 15 *Canadian Journal of Law and Technology* 121.

étrangers[239], faire l'objet de dispositions de portée générale sur les modalités de leur utilisation par des organismes publics en droit fédéral. La reconnaissance faciale automatisée dans les secteurs public et privé constitue désormais une réalité tangible en vue de la transition numérique des administrations publiques[240].

Dans les aéroports canadiens, le contrôle d'identité pour la déclaration électronique reste l'exemple le plus connu. En ce qui concerne l'utilisation de la reconnaissance faciale ou d'autres types de renseignements qui visent les citoyens canadiens, la *Loi sur l'Agence des services frontaliers* n'offre pas de précisions[241], ce qui permettrait de déduire que c'est le régime général de l'article 4 de la *Loi sur la protection des renseignements personnels* qui peut s'appliquer[242], en ce sens que l'Agence ne pourrait partager ce type d'information avec d'autres organismes fédéraux[243] ou d'autres États. Cette réserve est importante, car

239 Pour le processus d'immigration au Canada, l'obtention de renseignements biométriques est autorisée par la *Loi sur l'immigration et la protection des réfugiés*, L.C. 2001, c. 27, art. 10.01; L'application de cette loi par voie électronique est prévue par la partie 4.1 qui a été ajoutée en 2015. L'utilisation et la communication de renseignements biométriques, ainsi que les renseignements personnels, font l'objet de précisions supplémentaires dans la partie 2 du *Règlement sur l'immigration et la protection des réfugiés*, DORS/2002-227, art. 13.11; les renseignements obtenus sont communiqués à l'Agence des services frontaliers du Canada et à la Gendarmerie royale du Canada. Sur le sujet : AGENCE DES SERVICES FRONTALIERS DU CANADA, *Contrôle biométrique*, 2019, en ligne : < https://www.cbsa-asfc.gc.ca/security-securite/biometrics-biometrique-fra.html >; IMMIGRATION, RÉFUGIÉS ET CITOYENNETÉ CANADA, *Biométrie et protection des renseignements personnels*, 2019, en ligne : < https://www.canada.ca/fr/immigration-refugies-citoyennete/campagnes/biometrie/protection-renseignements-personnels-demandeur.html >.

240 BUREAU DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Reconnaissance faciale automatisée dans les secteurs public et privé*, Ottawa, 2013, en ligne : < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/fr_201303/ >.

241 *Loi sur l'Agence des services frontaliers du Canada*, L.C. 2005, c. 38.

242 *Supra*, note 155.

243 L'Agence des services frontaliers du Canada peut partager, éventuellement, au cas par cas, les informations recueillies avec l'Agence de santé publique du

la reconnaissance faciale a été mise en œuvre en 2017 par l'implantation des « bornes d'inspection primaire » (BIP) pour la déclaration électronique dans les aéroports canadiens[244]. Dans le cas des étrangers, l'échange automatisé de renseignements biométriques avec quelques États du Commonwealth (Australie, Nouvelle-Zélande et Royaume-Uni), ainsi qu'avec les États-Unis, fonctionne depuis quelques années sur la base de partenariats[245]. En revanche, les renseignements biométriques recueillis aux fins de l'application de la *Loi sur le précontrôle* ne peuvent être conservés par les contrôleurs américains et canadiens[246]. La dimension sécuritaire peut néanmoins favoriser le partage de données biométriques, car la délivrance du passeport canadien sous forme électronique permet de verrouiller et de conserver l'information par une puce[247]. L'information ainsi recueillie peut être transmise plus facilement dans le cas des individus recherchés par les autorités policières, ou encore, de ceux qui ont un casier judiciaire. Afin

Canada, ainsi qu'avec Emploi et Développement social Canada : AGENCE DES SERVICES FRONTALIERS DU CANADA, *Évaluation des facteurs relatifs à la vie privée de la borne d'inspection primaire*, 2017, en ligne : < https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-fra.html >.

244 L'Agence des services frontaliers du Canada précise qu'aucun renseignement personnel n'est stocké sur les bornes électroniques. Les renseignements recueillis sont cryptés et transférés vers ses fonds de renseignements. De façon plus subtile, le procédé de la chaîne de confiance renvoie aux utilisateurs le stockage des renseignements biométriques qui les concernent : AGENCE DES SERVICES FRONTALIERS DU CANADA, *Prototype de la chaîne de confiance*, 2018, en ligne : < https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/bp2020/2018/trust-confiance-fra.html >; pour utiliser le prototype de la chaîne de confiance, les voyageurs doivent télécharger une application sur leur téléphone intelligent et se créer un compte afin d'inclure un identificateur unique basé sur leurs données biométriques.

245 Ce sont des protocoles d'entente qui découlent du *Règlement sur l'immigration et la protection des réfugiés*, préc., note 239, partie 19.1 (« Échange de renseignements entre pays »), art. 315.21 et suiv.

246 *Loi sur le précontrôle*, L.C. 2017, C. 27, art. 33 (2).

247 GOUVERNEMENT DU CANADA, *Le passeport électronique*, 2017, en ligne : < https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens/centre-aide/passeport-electronique.html >. Dans quelques pays, la puce permet également l'enregistrement des empreintes digitales du titulaire du passeport. Au Canada, le seul élément biométrique est la photo numérisée du visage du titulaire.

d'assurer le respect des exigences de la *Loi sur la protection des renseignements personnels*, le Commissaire à la protection de la vie privée rappelle aux organismes fédéraux qu'il est nécessaire de faire une étude de gestion des risques (évaluation des facteurs relatifs à la vie privée)[248].

Au Québec, un procédé qui permet de saisir des caractéristiques ou des mesures biométriques ne peut être utilisé sans le consentement exprès de la personne visée. Le cas échéant, ces informations doivent être détruites si leur utilisation n'est plus justifiée, notamment après la vérification de l'identité de l'intéressé[249]. Le législateur a néanmoins permis la création d'une ou de plusieurs banques de renseignements biométriques qui seraient sujettes au contrôle de la Commission d'accès à l'information, celle-ci pouvant en déterminer les modes d'utilisation et de conservation[250]. Compte tenu des ambitions affichées par le gouvernement du Québec en matière de virage numérique, des modifications législatives seront nécessaires[251]. Les photos numérisées qui remplaceront inévitablement celles qui figurent actuellement sur les permis de conduire et les cartes d'assurance maladie feront surgir quelques problèmes dans la mesure où la reconnaissance faciale sera banalisée sur le plan technologique. *A priori*, faute de précautions, l'établissement de correspondances entre des renseignements contenus dans différentes bases de données (dont les finalités diffèrent) deviendrait possible. La reconnaissance faciale par l'usage d'un procédé technologique est désormais présente sur le marché puisque le public a la possibilité d'acheter des logiciels. Les images numérisées pourraient ainsi

248 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nos attentes : guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée*, Gatineau, 2020, en ligne : < https://priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/gd_exp_202003/ >.

249 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 44.

250 *Id*., art. 45.

251 Des modifications seront également nécessaires en Ontario malgré l'avancée que représente la *Loi de 2008 sur les cartes-photo*, L.O. 2008, c. 17. Les autorités peuvent utiliser une application logicielle qui permet de mesurer les caractéristiques du visage d'une personne (art. 7).

être décodées et intégrées par des logiciels dans d'autres banques de données publiques ou privées.

À ces interrogations, la *Loi concernant le cadre juridique des technologies de l'information* offre quelques réponses. Si la vérification de l'identité d'une personne peut être effectuée à partir « de caractéristiques qu'elle présente ou possède[252] », cette identité ne peut être « établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose[253] ». Comme le recommande le Commissaire à la vie privée du Canada, les photos numérisées ne doivent servir qu'à la vérification de l'identité d'une personne, en utilisant un autre mécanisme pour l'authentification afin d'accéder au dossier de la personne[254]. Malgré le fait que l'utilisation de caractéristiques ou de mesures biométriques aux fins d'identité reste interdit[255], le recours aux photos numérisées ne permet-il pas, en réalité, de saisir quelques-unes de ces caractéristiques? Les logiciels de numérisation du visage humain sont largement présentés comme des systèmes de reconnaissance et d'identification biométrique par l'industrie du numérique.

Afin de poursuivre cette réflexion, rappelons que le traitement de données biométriques « aux fins d'identifier une personne physique de manière unique » est interdit par l'article 9 du RGPD, sous réserve de onze exceptions[256]. Parmi celles-ci, le traitement de ce type de données serait nécessaire en vue de l'exécution des obligations et de l'exercice des droits en matière de droit du travail, de la sécurité sociale et de la protection

252 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 40 al. 2.

253 *Id*., art. 44.

254 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « *Des données au bout des doigts : la biométrie et les défis qu'elle pose à la protection de la vie privée* », Ottawa, 2011, en ligne : < https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/ >.

255 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 44.

256 RGPD, préc., note 25, art. 9 (1).

sociale[257]. Ce traitement peut également être requis pour des motifs d'intérêt public dans le domaine de la santé[258]. Enfin, le traitement des données qui relèvent de ces exceptions ne peut être fait que par un professionnel de la santé soumis à une obligation de secret professionnel. Un exemple récent venant de la France montre que le juge administratif peut censurer, sur le fondement de l'article 9 du RGPD, l'utilisation de la reconnaissance faciale pour la simple surveillance, notamment à titre de complément ou de substitut à la vidéosurveillance[259].

III. L'importance grandissante des algorithmes dans les procédures administratives automatisées

La définition la plus courante de l'algorithme le présente comme « un ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations », ce qui entraîne sa transposition en langage de programmation exécutable par un ordinateur[260]. Comme le montre la racine grecque, *arithmos* (« nombre »), les algorithmes sont associés à la mesurabilité et à la quantification. Les plus connus sont ceux qui permettent la compression de données, le tri, la cryptographie, les graphes, ainsi que des opérations qui relèvent du graphisme, du génie logiciel, des mathématiques, notamment aux fins d'optimisation pour les systèmes de calcul formel[261].

Dans les administrations publiques, l'utilisation des algorithmes peut être liée à des fonctions de recherche en vue de simulation et de

257 *Id*., art. 9 (2) b.

258 *Id*., art. 9 (2) i.

259 Dans une décision rendue le 27 février 2020, la délibération du Conseil régional de Provence-Alpes-Côte d'Azur qui autorisait l'expérimentation d'un dispositif de reconnaissance faciale dans deux lycées, à Marseille et à Nice, a été annulée pour motif d'incompétence, mais également pour atteinte aux exigences de l'article 9 du RGPD : *Association La Quadrature du Net et autres*, nº 1901249, TA Marseille, 27 février 2020, (commentaire de Jean-Marc PASTOR, « Pas de reconnaissance faciale dans un lycée », (2020) 9 AJDA 492).

260 *Dictionnaire Larousse*, s.v. « Algorithme », en ligne : < www.larousse.fr >.

261 « Liste des algorithmes », *Scriptol*, en ligne : < https://www.scriptol.fr/programmation/liste-algorithmes.php >.

projection. Statistique Canada peut ainsi analyser des bases de données afin d'obtenir différents modèles de simulation de politique sociale[262]. Les informations consultables auprès de Statistique Canada montrent leur importance dans l'analyse des soins de santé, de l'indice du chômage, de la transmission intergénérationnelle du revenu, de l'évolution de plusieurs types de cancer, des enjeux pour la santé et la sécurité au travail, pour ne donner que quelques exemples. Les juristes seront plus directement interpellés par l'utilisation des algorithmes dans l'analyse de l'activité judicaire, spécialement dans le domaine de la justice pénale[263]. Compte tenu des possibilités offertes en fait de simulation et de projection, l'évaluation algorithmique est susceptible de compléter le recours aux études d'impact en matière réglementaire. Elle peut potentiellement jouer un rôle déterminant dans l'élaboration des politiques publiques. La dimension juridique a déjà été soulignée pour la protection des données.

Pour le traitement de celles-ci, les algorithmes offrent des possibilités de conversion vers l'anonymisation et le cryptage. Malgré cet usage très répandu, les algorithmes sont davantage associés à l'atteinte d'un résultat qui a une fonction prédictive. En France, les systèmes algorithmiques d'aide à la décision, partiellement ou entièrement automatisés, sont de plus en plus répandus dans le domaine médical et sanitaire, policier, judiciaire, ainsi que dans divers champs de l'action administrative (enseignement, aide sociale, emploi et fiscalité)[264]. Ces systèmes peuvent être utilisés dans le but d'obtenir un résultat tangible qui peut être comparé

---

262 STATISTIQUE CANADA, *Base de données et modèle de simulation de politique sociale* (BD/MSPS), Ottawa, 2020, en ligne : < https://www150.statcan.gc.ca/n1/fr/catalogue/89F0002X >.

263 Cristine ROTENBERG, « De l'arrestation à la déclaration de culpabilité : décisions rendues par les tribunaux dans les affaires d'agression sexuelle déclarées par la police au Canada, 2009 à 2014 », Ottawa, Statistique Canada, 2017, en ligne : < https://www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/54870-fra.htm >.

264 Sonia DESMOULIN-CANSELIER et Daniel LE MÉTAYER, *Décider avec les algorithmes. Quelle place pour l'Homme, quelle place pour le droit?*, Coll. « Les Sens du droit », Paris, Dalloz, 2020, chap. 1, p. 23 et suiv.; Danièle BOURCIER et Primavera DE FILIPPI, « Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage? », (2018) 167 *Revue française d'administration publique* 525.

à une décision administrative. Plusieurs processus administratifs reposent sur l'analyse de faits quantifiables en vue de rendre une décision. Cette quantification peut devenir très importante si des dimensions biométriques sont requises pour déterminer le montant d'une prestation ou d'une indemnisation.

A) Le droit administratif à l'épreuve de la rationalité algorithmique

Dans la perspective du droit administratif, le recours à des algorithmes exige des nuances. Si un algorithme permet d'accélérer le calcul et le tri, il offre également une fonction de synthèse qu'un processus administratif « classique » ne permet pas d'atteindre. La combinaison simultanée de données quantifiables est de plus en plus répandue pour des opérations qui ne relèvent pas du droit. Pensons, à titre d'exemple, en matière d'activité sportive, à la plongée en eau profonde : dans ce cas, les ordinateurs fonctionnent avec un algorithme de décompression[265].

La décision administrative classique résulte d'une logique causale et cumulative par addition des éléments dans l'analyse d'un dossier. Cette évaluation ne sera plus la même avec une logique de synthèse informatique. Les algorithmes contemporains « opèrent selon une logique de corrélations statistiques et selon une logique probabiliste plutôt que selon une logique

265 Ces ordinateurs sont minimalement équipés d'un profondimètre, d'un chronomètre, d'un thermomètre et d'un compas. Ils indiquent ainsi la profondeur, le temps de plongée et, surtout, la vitesse de remontée (généralement autour de 10 mètres par minute), le temps de non-décompression, suivi, habituellement, d'une durée limitée de quelques minutes de décompression avant de revenir à la surface. Le résultat (temps de décompression/nombre d'heures requis avant de prendre l'avion) ressemble à bien des égards à une « décision » qui devient aussi contraignante, sinon davantage, que celle qui est issue d'un processus administratif obéissant à des balises juridiques, car le plongeur ne peut pas vraiment s'y soustraire sans risquer de graves lésions corporelles. Cette « décision » est fonction du résultat offert par un algorithme de décompression : Drew RICHARDSON (dir.), *The Encyclopedia of Recreational Diving*, 3e éd., Rancho Santa Margarita (CA), PADI, 2008, p. 5-64 (« Dive Computers »).

causale et déterministe[266] » qui sont très différentes, à bien des égards, du raisonnement juridique. Un algorithme offre des possibilités de synthèse avancée dans la mesure où il peut, par exemple, intégrer des résultats médicaux et des données biométriques avec plusieurs bases de données résultant de l'action administrative (banque de décisions) et de l'activité de diverses catégories de cours et de tribunaux (banque de jurisprudence).

Faut-il déduire de cette évolution l'apparition d'un droit des décisions administratives automatisées[267]? Si ce scénario est esquissé en France, il est encore plus explicite en droit américain[268], même si l'automatisation peut parfois devenir un objet de controverses[269]. Au Canada, et de façon plus spécifique au Québec, les sites Web des organismes publics offrent encore peu d'information sur l'usage des algorithmes, en dépit du fait que leur utilisation soulève plusieurs questions importantes pour le droit administratif. Les autorités fédérales reconnaissent explicitement le phénomène de la « décision automatisée » puisque la *Directive sur la prise de décision automatisée* est diffusée depuis 2019[270].

---

266 Jean-Bernard AUBY, « Le droit administratif face aux défis du numérique », (2018) 15 *AJDA* 835, 843.

267 Judith ROCHFELD, « L'encadrement des décisions prises par algorithme », dans Stéphane PRÉVOST et Erwan ROYER, *Intelligence artificielle*, Coll. « Grand Angle », Paris, Dalloz, 2019, p. 11, à la p. 15 (« Vers un droit des décisions automatisées? »); Jean-Baptiste DUCLERC, « L'automatisation algorithmique des décisions administratives individuelles », (2019) *Revue du droit public* 313.

268 Cary COGLIANESE et Lavi M. BEN DOR, «AI in Adjudication and Administration», (2020) *Penn Law: Legal Scholarship Repository* 2118, en ligne : < https://scholarship.law.upenn.edu/faculty_scholarship/2118 >; Cary COGLIANESE et David LEHR, « Regulating by Robot: Administrative Decision Making in the Machine-Learning Era », (2017) 105-5 *Georgetown Law Journal* 1147, 1160 (« Existing Administrative Applications »); Mariano-Florentino CUÉLLAR, « Cyberdelegation and the Administrative State », dans Nicholas R. PARILLO (dir.), *Administrative Law from the Inside out: Essays on Themes in the Work of Jerry L. Mashaw*, Cambridge, Cambridge University Press, 2017, 134.

269 Danielle KEATS CITRON et Ryan CALO, « The Automated Administrative State: A Crisis of Legitimacy », (2020), en ligne : < https://scholarship.law.bu.edu/faculty_scholarship/838 >.

270 GOUVERNEMENT DU CANADA, *Directive sur la prise de décision automatisée*, 2019, préc., note 7, cette directive est en vigueur depuis avril 2020.

Cette directive rappelle que les décisions automatisées doivent être « conformes à l'équité procédurale et aux exigences d'application régulière de la loi » (art. 4.2.1). Aux fins de transparence, elle oblige les organismes fédéraux à « publier par l'entremise des sites Web pertinents des avis sur le fait que la décision rendue sera formulée totalement ou en partie par un système automatisé » (art. 6.2.1). Dans le projet de loi C-11 (qui ne vise pas les institutions fédérales), le législateur propose une définition générique pour décrire ce que représente un « système décisionnel automatisé » compte tenu de l'objet et du champ d'application de ce projet relatif à la vie privée des consommateurs[271]. Il s'agit du traitement des renseignements personnels par les organisations qui font du commerce électronique, ce qui ne correspond pas, au niveau des principes, au type de travail que font les administrations publiques afin de rendre des décisions.

Par le dépôt du projet de loi nº 64, le Québec reconnaît également l'existence de la « décision fondée exclusivement sur un traitement automatisé ». Notons que la personne visée doit être informée de l'automatisation. Si elle en fait la demande, l'organisme public doit l'informer des renseignements personnels qui ont été utilisés mais, surtout, « des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision[272] ». Dans la perspective du droit à la motivation des décisions administratives, c'est un ajout important. De façon plus générale, les réformes en cours privilégient la reconnaissance d'un « droit à l'explication » lorsqu'il s'agit d'une prédiction, d'une recommandation ou d'une décision[273].

---

271 « Système décisionnel automatisé » : Technologie qui appuie ou remplace le jugement de décideurs humains au moyen de techniques telles que l'usage de systèmes basés sur des règles, l'analyse de régression, l'analytique prédictive, l'apprentissage automatique, l'apprentissage profond et l'usage de réseaux neuronaux; *Loi de 2020 sur la mise en œuvre de la Charte du numérique*, Projet de loi C-11, préc., note 11.

272 Projet de loi nº 64, préc., note 145, art. 20 (ajout de l'article 65.2 à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24).

273 *Loi de 2020*, préc., note 11, par. 63 (3). Malgré le fait que ce soit un environnement numérique, le projet de loi prévoit que cette demande d'explications soit présentée par écrit : par. 64 (1).

Au-delà du droit canadien, l'article 22 du RGPD interdit l'élaboration d'une décision fondée exclusivement sur un traitement automatisé, sous réserve de quelques exceptions, notamment si ce traitement est autorisé par le droit de l'Union européenne ou d'un État membre, ou encore, avec le consentement explicite de la personne visée[274]. Dans la perspective du droit canadien, les exigences de l'équité procédurale requièrent, à tout le moins, l'examen individualisé d'un dossier en vue de rendre une décision, en particulier si les répercussions sont importantes pour la personne intéressée[275]. De façon plus subtile, la réponse dépend du rôle attribué à l'algorithme dans un processus décisionnel. Lorsqu'un pouvoir discrétionnaire est accordé par la loi, il doit être exercé[276]. Ce principe très connu a néanmoins fait l'objet d'aménagements compte tenu de l'utilisation des directives, des politiques et des lignes directrices pour faciliter l'évaluation des dossiers par des règles générales[277]. Dans ce cas de figure, l'utilisation d'un algorithme ne peut être exclue d'emblée si un agent vérifie d'abord que la personne intéressée répond aux exigences de la loi pour le traitement de son dossier (étape préliminaire) et qu'il utilise ensuite un procédé algorithmique afin de déterminer, le cas échéant, le montant attribué à titre d'allocation, de prestation ou d'indemnité. L'aspect qui

274 RGDP, préc., note 25, art. 22 (1) et (2). Depuis 1978, la législation française prévoit « qu'aucune […] décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité » : *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. du 7 janvier 1978, art. 10 (avec une exception pour les décisions prises dans le contexte de la conclusion ou de l'exécution d'un contrat).

275 *Baker* c. *Ministre de la Citoyenneté et de l'Immigration du Canada*, [1999] 2 R.C.S. 817, par. 25 et 43. Cette analyse a été proposée en droit américain : Danielle KEATS CITRON, « Technological Due Process », (2008) 85-6 *Washington Law Review* 1249.

276 Pierre ISSALYS et Denis LEMIEUX, *L'action gouvernementale. Précis de droit des administrations publiques*, 4e éd., Montréal, Éditions Yvon Blais, 2020, p. 223 (« Le refus d'exercice d'un pouvoir discrétionnaire »). Le tirage au sort peut être autorisé expressément par règlement, notamment dans le domaine de la chasse : *Règlement sur la chasse*, RLRQ, c. C-61.1, r. 12, art. 7.1.

277 D. MOCKLE, « Politiques, directives et instruments de gestion », préc., note 55, par. 34 (« Pouvoir discrétionnaire et directive »).

relève encore de l'incertitude est l'utilisation exacte qu'en font les administrations publiques[278]. Le portrait se révèle un peu plus précis pour l'administration fédérale américaine[279]. Suivant des règles connues pour l'utilisation des directives, celles-ci ne peuvent pas être appliquées de façon rigide ou automatique afin de tenir compte, le cas échéant, des particularités d'un dossier[280]. Cette exigence est-elle compatible avec l'uniformité de traitement associée à l'usage des algorithmes? L'agent responsable d'un dossier peut-il procéder autrement dans l'analyse d'un dossier sans porter atteinte à la cohérence algorithmique? Compte tenu du fait que plusieurs algorithmes sont de type déterministe en facilitant le classement et le tri, leur usage relève, de prime abord, de l'exercice d'une compétence liée.

La transparence constitue un enjeu important. La première étape consiste à informer le public de l'existence et de l'utilisation d'un algorithme aux fins d'un processus décisionnel. À titre comparatif, la France en offre un exemple puisque le Code des relations entre le public et l'administration (2015) prévoit que toute « décision individuelle prise sur le fondement algorithmique comporte une mention explicite en informant l'intéressé ». Sur le plan de la motivation, la même disposition précise que « les règles définissant ce traitement et les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande »[281]. Certes, ce droit d'accès ne permet pas d'obtenir

278 Une analyse des usages et des pratiques au sein des organismes fédéraux a été entreprise en 2019 par questionnaire (« Évaluation de l'incidence algorithmique ») en vue d'assurer une application éthique et responsable de l'intelligence artificielle : en ligne : < https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/evaluation-incidence-algorithmique.html >.

279 David FREEMAN ENGSTROM et autres, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, *Report submitted to the Administrative Conference of the United States*, 2020, en ligne : < https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf >.

280 P. ISSALYS et D. LEMIEUX, préc., note 276, p. 737 (« L'application nuancée de la directive »).

281 *Code des relations entre le public et l'administration*, 4e éd., Dalloz, 2020, art. L. 311-3-1 : ce code a été créé par l'ordonnance no 2015-1341 du 23 octobre 2015, J.O. 25 octobre 2015, p. 19872, et il est en vigueur depuis le 1er janvier 2016.

directement le contenu de l'algorithme, mais il offre néanmoins la possibilité d'avoir de l'information sur son utilisation. Cet ajout s'avère important, car l'évaluation de la portée des algorithmes est requise pour une meilleure compréhension de la motivation des décisions administratives[282]. Au Canada, la *Directive sur la prise de décision automatisée* oblige depuis 2019 tout organisme ou tout ministère à « fournir une explication significative aux personnes concernées sur la façon dont la décision a été prise et la raison pour laquelle elle a été prise » (art. 6.2.3)[283]. Par le dépôt du projet de loi nº 64, le Québec reconnaît que la personne visée peut obtenir les raisons, ainsi que les principaux facteurs et paramètres, ayant mené à la décision[284]. Le terme « paramètre » est-il suffisamment précis pour viser le degré et le mode de contribution algorithmique à la prise de décision? Pour clarifier cet élément, la Commission d'accès à l'information assure un rôle de surveillance en vue de l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[285]. Les organismes publics sont tenus de transmettre toute information qu'elle requiert afin d'assurer l'application de cette loi[286].

L'article L. 311-3-1 est complété par une disposition réglementaire qui précise que, en cas de demande de communication, l'administration doit fournir « sous une forme intelligible […] (1) Le degré et le mode de contribution algorithmique à la prise de décision; (2) Les données traitées et leurs sources; (3) Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé; (4) Les opérations effectuées par le traitement » : *Décret nº 2015-1342 du 23 octobre 2015*, J.O. 25 octobre 2015, p. 19895, art. R.311-3-1-2. Ces dispositions qui n'étaient pas dans la version initiale du Code ont été introduites par la *Loi nº 2016-1321 du 7 octobre 2016 relative à une République numérique*, ainsi que par décret pour le volet réglementaire : *Décret nº 2017-330 du 14 mars 2017*.

282 Daniel MOCKLE, « La motivation des actes administratifs au Canada », (2019) 17 *Cahiers de la recherche sur les droits fondamentaux* 125, 136 (« La nécessité d'un cadre législatif »).

283 GOUVERNEMENT DU CANADA, préc., note 7.

284 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, préc., note 145, art. 20.

285 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 24, art. 122.1.

286 *Id*., art. 130.

Dans une perspective de transparence, le législateur emprunte ainsi le cadre juridique de l'accès à l'information pour offrir une première garantie en matière de décision automatisée, alors qu'en contrepartie, la *Loi sur la justice administrative* prévoit la motivation obligatoire des décisions de refus à l'occasion de l'exercice d'une fonction administrative[287]. Par sa portée, le projet de loi nº 64 reconnaît un droit plus général en matière de décision automatisée. En effet, le champ d'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* est plus vaste que celui de la *Loi sur la justice administrative*[288].

Cet exemple illustre les avantages de la codification uniforme de la procédure administrative non contentieuse. Le Canada, sur le plan du droit fédéral, offre un net contraste par rapport au mouvement général de codification dans ce domaine[289]. À l'instar de la Grande-Bretagne, c'est l'un des rares pays à ne pas avoir de législation sur ce sujet. En dépit de sa proximité géographique avec les États-Unis, il n'a élaboré aucune loi de portée générale comparable à l'*Administrative Procedure Act* de 1946 avec ses modifications subséquentes[290]. Le Canada n'en reste pas moins un État

---

287 *Loi sur la justice administrative*, RLRQ, c. J-3, art. 8.

288 Pour l'application des articles 2 à 8, la *Loi sur la justice administrative*, préc., note 287, art. 3, ne vise que l'Administration gouvernementale qui est constituée de ministères et organismes gouvernementaux dont le gouvernement ou un ministre nomme la majorité des membres et dont le personnel est nommé suivant la *Loi sur la fonction publique*, RLRQ, c. F.3.1.1.

289 Jean-Bernard AUBY et Thomas PERROUD (dir.), *Droit comparé de la procédure administrative/Comparative Law of Administrative Procedure*, Bruxelles, Bruylant, 2016, p. 9 (« Introduction » par Michel Fromont); Jacques ZILLER, Jens-Peter SCHNEIDER et Herwig HOFMANN (dir.), *La codification de la procédure administrative de l'Union européenne. Le modèle ReNEUAL*, Bruxelles, Bruylant, 2017.

290 Ce constat doit être nuancé puisque des tentatives de codification de la procédure administrative ont été proposées, notamment celle qui a été suggérée en 1985 par la défunte Commission de réforme du droit pour les organismes administratifs autonomes, ainsi que celle qui a été lancée en 1995 par le ministère de la Justice du Canada, et qui n'ont connu aucune suite : COMMISSION DE RÉFORME DU DROIT DU CANADA, *Les organismes administratifs autonomes/Independant Admi-*

fédéral où quatre provinces ont adopté des lois de procédure qui visent le fonctionnement des tribunaux administratifs, ainsi que des dimensions plus générales de procédure administrative non contentieuse[291]. Parmi celles-ci, le Québec occupe une place relativement originale avec la *Loi sur la justice administrative*, où la distinction entre les décisions prises dans l'exercice d'une fonction administrative et celles qui le sont dans l'exercice d'une fonction juridictionnelle a permis de reconnaître l'existence de garanties procédurales propres à la procédure non contentieuse[292]. Si cette ouverture reste modeste en comparaison de ce qui a été fait ailleurs, elle ouvre néanmoins des perspectives sur la codification du droit administratif.

Le corpus législatif peut être ainsi modifié de diverses manières par l'ajout de dispositions relatives aux enjeux numériques. Le cas échéant, une loi de transition numérique peut offrir un cadre conceptuel plus spécifique. Peu de temps après l'entrée en vigueur de l'*E-Government Act* de 2002, l'Italie a adopté un code de l'administration numérique (Codice dell'aministrazione digitale) qui compte neuf chapitres[293]. Par ses finalités et son objet, ce code – qui date de 2005 – vise avant tout le passage de l'administration publique au numérique avec un très grand niveau de généralité dans l'énoncé des principes. La création d'une agence (Agenzia per l'Italia digitale) rend toutefois cet objectif plus réaliste[294]. En mettant

nistrative Agencies, Rapport 26, Ottawa, CRDC, 1985. Ces propositions ne visaient pas explicitement la procédure administrative non contentieuse.

291 L'Alberta a élaboré des règles procédurales en 1966 (*Administrative Procedures and Jurisdiction Act*, SA 1966, c. 1; RSA 2000, c. A-3). La législation de l'Ontario (*Loi sur l'exercice des compétences légales/Statutory Powers Procedure Act*, L.O. 1993, c. 27; L.R.O. 1990, c. S-22) et celle de la Colombie-Britannique (*Administrative Tribunals Act*, S.B.C. 2004, c. 45) ne visent que les tribunaux administratifs.

292 *Loi sur la justice administrative*, préc., note 287, art. 2-8.

293 *Codice dell'amministrazione digitale*, Décret législatif du 7 mars 2005, nº 82, avec modifications subséquentes, en ligne : < https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2018-09-28/index.html >.

294 L'Agenzia per l'Italia digitale a pris la relève en 2012 (Décret législatif du 22 juin 2012, nº 83, converti en loi le 7 août 2012) de l'Agence pour la diffusion des technologies de l'innovation : en ligne : < https://www.agid.gov.it >.

sur pied Infrastructures technologiques Québec en 2020[295], les autorités québécoises ont également privilégié une formule de type « agence ».

Si la transition numérique des administrations publiques ne peut se faire uniquement par la loi, le recours à la législation permet de reconnaître des droits et des garanties aux citoyens, aux organisations et aux entreprises. Pour ce qui est du droit fédéral, l'approche canadienne est d'un tout autre type, car elle privilégie « l'expérience du client » avec l'utilisation de politiques et de directives, ce qui rejoint le type managérial[296]. Malgré le fait que les autorités fédérales n'aient pas cherché à éluder le phénomène de la « prise de décision automatisée », la réponse offerte ne convient pas puisque les principaux enjeux sont limités à la sphère administrative. Même si l'objectif est de « veiller à la transparence et à la divulgation de renseignements concernant l'utilisation de ces systèmes, ainsi qu'à l'évaluation et la gestion continue des risques[297] », les autorités fédérales ont pour principal objectif le fonctionnement des ministères et des organismes fédéraux. Si la législation québécoise se limite au rappel du principe de transparence[298], elle sera, selon toute vraisemblance, modifiée par l'adoption du projet de loi nº 64[299].

Sur le plan des principes, la loi offre l'avantage de la cohérence, de la simplicité et d'une relative centralisation de l'information. À titre d'exemple, le Code des relations entre le public et l'administration (France) a permis d'élaborer des « règles particulières à la saisine et aux échanges par voie électronique », de même que d'autres modalités lorsqu'une consultation est ouverte sur Internet[300]. Cette unité évite la fragmentation

295 *Loi visant principalement à instituer le Centre d'acquisitions gouvernementales et Infrastructures technologiques Québec*, préc., note 3.

296 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *Politique sur les services et le numérique*, préc., note 7, art. 3.1.1.

297 *Id*., art. 4.4.2.4.2.

298 *Loi favorisant la transformation numérique de l'administration publique*, préc., note 2, art. 1; *Loi sur l'administration publique*, préc., note 57, art. 1.

299 Projet de loi nº 64, préc., note 145.

300 *Code des relations entre le public et l'administration*, préc., note 281, art. L-112-1–R-112-20, L-132-1 (complété par les articles R-132-7 à R-132-10 du règlement d'application du Code).

qui résulterait de la modification de plusieurs lois dans divers champs de l'action administrative, notamment dans le domaine de l'environnement[301]. Les choix restent néanmoins difficiles, car une loi générale de transition numérique aurait pour effet de modifier plusieurs lois préexistantes.

Si le recours à un cadre législatif permet de satisfaire à des exigences largement connues en droit administratif (transparence, garanties procédurales, motivation des décisions administratives), son but premier ne vise pas la réglementation des algorithmes. En droit américain, un expert du ministère de la Justice a proposé en 2017 la création d'une agence fédérale inspirée du modèle offert par la *Food & Drug Administration* (FDA) afin de remédier à des problèmes similaires liés à l'utilisation des algorithmes[302]. Son argumentaire vise avant tout l'essor des algorithmes d'apprentissage (*machine-learning algorithms*) dont l'opacité et la complexité sont à l'origine de risques réels en termes de dangerosité et de responsabilité, au même titre que l'élaboration de nouveaux médicaments. Dans cette perspective, une agence fédérale aurait un rôle déterminant à des fins de contrôle et de réglementation (*standards-setting body*), notamment à des fins de classification des algorithmes et d'élaboration de standards (*Performance standards, Design standards, Liability Standards*). Suivant sur ce point un argumentaire largement connu en Amérique du Nord pour le droit public, la création de cette agence répondrait à la nécessité de baliser l'usage des algorithmes par un organisme indépendant ayant une réelle expertise scientifique et technique. Deux chercheurs canadiens ont repris cette solution (*a Canadian Regulatory Agency*) afin de répondre à des exigences de transparence et d'imputabilité, mais également afin de remédier à des problèmes de discrimination *(eliminate or control discriminatory and biased algorithm behavior*)[303]. Si ces interrogations

301 Au Québec, le Bureau d'audiences publiques sur l'environnement peut, depuis 2017, adopter des règles qui « doivent notamment prévoir des modalités régissant la participation du public par tout moyen technologique approprié » : *Loi sur la qualité de l'environnement*, RLRQ, c. Q-2, art. 6.6.

302 Andrew TUTT, « An FDA for Algorithms », (2017) 69 *Administrative Law Rev*. 83.

303 Robert A. SMITH et Pierre R. DESROCHERS, « Should algorithms be regulated by government? », (2020) 63 *Canadian Public Administration / Administration*

visent à trouver des solutions *ex ante* dès le stade de la conception, il ne faut pas perdre de vue que c'est l'usage qui reste déterminant.

Sur ces questions, les positions réciproques des États-Unis et de l'Union européenne ne sont pas du même type. Du côté américain, la *National Artificial Intelligence Initiative Act* a été adoptée en mars 2020[304]. Sous la dénomination générale d'une orientation (*Initiative*), son but premier est de reconnaître le rôle prépondérant du Gouvernement fédéral en matière de recherche, de développement, de financement et d'élaboration de règles, avec la perspective de favoriser une meilleure coordination de tous les acteurs concernés en matière d'intelligence artificielle. La création d'un comité directeur à des fins d'expertise (*National Artificial Intelligence Advisory Committee*) a été prévue, ainsi que celui d'un office (*National Artificial Intelligence Initiative Office*) afin de mettre en œuvre cette « initiative ». Pour l'encadrement normatif, cette loi évoque simplement le support requis des autorités fédérales pour l'élaboration de normes volontaires et de bonnes pratiques[305].

Les Européens abordent ces enjeux dans une perspective très différente. En avril 2021, la Commission européenne a rendu public un projet de règlement à l'attention du Parlement européen et du Conseil afin d'établir des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle)[306]. La Commission justifie ce règlement par la nécessité de règles uniformes afin de mettre en place « un

publique du Canada 563. Si ce texte analyse un nombre important de publications américaines, il tient compte également des perspectives offertes par le *Règlement général sur la protection des données* (RGPD), préc., note 25.

304 *National Artificial Intelligence Initiative Act of 2020*, H.R. 6216, 116th Congress, 2e session, en ligne : https://www.congress.gov/bill/116th-congress/house-bill/6216.

305 *Idem,* par. 101, b, (2).

306 Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, COM (2021) 206, 21 avril 2021, en ligne : https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF.

marché unique pour des systèmes d'IA licites, sûrs et dignes de confiance »[307]. Le règlement offrira des règles relatives à l'interdiction de certaines pratiques préjudiciables reposant sur l'IA, ainsi que la classification de plusieurs systèmes d'IA. Il aura notamment pour effet d'introduire des exigences fondamentales pour les systèmes d'IA classés à haut risque. Comme il s'agit d'un règlement, son applicabilité sera directe dans tous les États membres de l'Union européenne. Le texte est précédé d'un important dispositif de considérants (89 au total). Pour l'élaboration de définitions précises de plusieurs termes, il offre un grand intérêt[308].

Le futur règlement européen offre ample matière à réflexion pour le Canada. À un tout autre niveau, les autorités fédérales ne sont pas restées inactives aux fins de la transition numérique de l'administration fédérale. Dans la *Politique sur les services et le numérique* de 2020, le secrétaire du Conseil du Trésor a la responsabilité d'établir et de présider « un organisme de niveau supérieur » afin de proposer des conseils et des recommandations, notamment pour les « Normes numériques du gouvernement du Canada » qui ont pour objet la gestion des données, la technologie de l'information et la cybersécurité[309]. Si cette orientation constitue un pas dans la bonne direction, elle est néanmoins révélatrice de la faiblesse du cadre juridique car cet organisme supérieur n'est pas indépendant et reste dépourvu de statut juridique. Dans la *Directive sur la prise de décision automatisée*, les autorités fédérales ont prévu « une évaluation de l'incidence algorithmique avant la production de tout système décisionnel automatisé », notamment afin de « s'assurer de l'absence de biais[310] imprévus dans les données et d'autres facteurs qui pourraient influencer injustement les résultats »[311]. Mais ici également, il n'y a pas d'évaluation externe. Ces exigences relèvent du sous-ministre adjoint responsable du système décisionnel ou de toute autre personne nommée par l'administrateur général[312].

307 I*dem*, Exposé des motifs, 2.4 (Choix de l'instrument).
308 Ibidem, titre I, art. 3 (Définitions).
309 *Politique sur les services et le numérique*, préc., note 7, art. 4.1.1.1.
310 Traduction littérale de *bias* afin d'exprimer l'idée de préjugés.
311 *Directive sur la prise de décision automatisée*, préc., note 7, art. 6.1.1.
312 *Id.*, art. 6.

B) Les garanties disponibles aux fins de contestation

Compte tenu de l'importance grandissante des algorithmes aux fins de décision administrative automatisée (en tout ou en partie), il est utile de vérifier si la législation québécoise, en son état actuel, offre des garanties minimales en matière de contestation de ce type de décisions. La *Loi sur la justice administrative* précise que les décisions qui relèvent de l'exercice d'une fonction administrative « sont conduites dans le respect du devoir d'agir équitablement » et que les décisions défavorables doivent être motivées[313]. Avant que le Tribunal administratif du Québec (TAQ) soit saisi d'une requête en contestation, les règles générales relatives à l'équité procédurale peuvent s'appliquer. Ces dernières ont été élaborées de manière à prendre en considération « l'importance de la décision pour les personnes privées », sans par ailleurs préciser le contenu pratique de la motivation si celle-ci est requise[314]. Pour les exigences de la motivation, la Cour suprême a amorcé un mouvement de repli depuis 2011 en affirmant que des revendications liées à l'exhaustivité des motifs, ou encore à leur insuffisance, ne permettent pas à elles seules de casser une décision[315]. Cette position a été confirmée dans l'affaire *Vavilov*[316].

Dans la phase ultérieure de la contestation devant le TAQ, celui-ci peut requérir de l'autorité administrative dont la décision est contestée la transmission du dossier[317]. Cette obligation est formulée en des termes généraux, mais le TAQ peut subordonner la recevabilité de la preuve à des règles de communication préalable[318]. L'avis de la Commission d'accès à l'information pourrait-il être envisagé à la lumière des transformations

313 *Loi sur la justice administrative*, préc., note 287, art. 2 et 8.

314 *Baker* c. *Ministre de la Citoyenneté et de l'Immigration du Canada*, préc., note 255, par. 25 et 43.

315 *Newfoundland and Labrador Nurses' Union* c. *Conseil du Trésor de Terre-Neuve-et-Labrador*, 2011 CSC 62, par. 16 et 17. Sur ce repli : Kendrick LO, « When Efficiency Calls: Rethinking the Obligation to Provide Reasons for Administrative Decisions » (2018) 43-2 *Queen's Law Journal* 325.

316 *Canada (Ministre de la Citoyenneté et de l'Immigration)* c. *Vavilov*, 2019 CSC 65, par. 91.

317 *Loi sur la justice administrative*, préc., note 287, art. 114 et 114.1.

318 *Id*., art. 138.

annoncées dans le projet de loi nº 64[319]? Si l'on compare les pouvoirs du TAQ avec ceux des cours judiciaires, l'utilisation du *Code de procédure civile* offre, à certains égards, plus de possibilités[320]. Cependant, le TAQ peut-il vraiment se prévaloir ainsi des pouvoirs généraux attribués aux juges et aux tribunaux de l'ordre judiciaire par le moyen de l'article 49 du *Code de procédure civile*[321]? Dans la perspective d'une demande de contrôle judiciaire dirigée contre une décision administrative, les juges ont beaucoup plus de pouvoirs. Pour la communication d'un élément de preuve en possession de l'une des parties, l'article 251 du *Code de procédure civile* offrirait une solution dans l'éventualité où un organisme public serait réticent à divulguer les modalités d'utilisation d'un algorithme. Le scénario de cette disposition vise toutefois un « élément matériel de preuve », ce qui oblige à réfléchir davantage sur le statut juridique des algorithmes.

Dans la mesure où les algorithmes sont très variés dans leur fonctionnement et leurs finalités, une clarification générale de leur statut paraît illusoire. En ce qui concerne le droit administratif, la situation est néanmoins différente. Un algorithme pouvant servir de fondement à un processus de décisions automatisées, en tout ou en partie, il représente dès lors « un niveau normatif clandestin », car la mise en œuvre de la législation devient alors tributaire d'un dispositif juridique qui y est intégré[322]. Il se transforme ainsi en une sorte de quasi-législation qui peut rejoindre d'autres procédés de substitution de l'action réglementaire « classique » sous forme

319 Projet de loi nº 64, préc., note 145.

320 En l'absence de dispositions applicables à un cas particulier, le TAQ peut suppléer par toute procédure compatible avec la loi ou ses règles de procédure : *Loi sur la justice administrative*, préc., note 287, art. 108. Il peut utiliser par analogie les dispositions du *Code de procédure civile*.

321 Aux fins de l'article 108, seuls des cas exceptionnels seraient considérés : Denis LEMIEUX, *Justice administrative. Loi commentée*, 3e éd., Brossard, Publications CCH, 2009, p. 197.

322 Dans une perspective de droit comparé, cette hypothèse a été soulevée par J.-B. AUBY, préc., note 266, p. 843, sur le fondement des travaux de Dag WIESE SCHARTUM, « Law and Algorithms in the Public Domain », (2016) 10 *Etikk i Praksis: Nordic Journal of Applied Ethics* 15.

de règlements[323]. Comme le souligne Jean-François Auby, « la gouvernance algorithmique pourrait engendrer une sorte de pouvoir réglementaire caché[324] ». Dans cette perspective, il est peu probable que l'on puisse utiliser la notion de directive telle qu'elle a été élaborée en droit administratif, notamment au Québec[325]. Ce procédé n'a de sens que si des dérogations sont possibles, ce qui semble peu compatible avec l'uniformité et la cohérence de la rationalité algorithmique. Cependant, tout est affaire de contexte. Si un agent peut soustraire l'évaluation d'un dossier à un traitement algorithmique afin de tenir compte de ses particularismes, le rapprochement avec la notion de directive serait plus réaliste : mais pourrait-il soustraire ce dossier sans avoir prévu le résultat potentiel (la décision) en utilisant l'algorithme destiné à l'évaluation de tous les dossiers? À ces interrogations s'ajoute le fait que plusieurs algorithmes ne sont pas dénués de capacité d'apprentissage[326], ce qui rend plus aléatoire la comparaison avec des notions classiques du droit administratif.

Dans cette perspective, les modalités d'utilisation d'un algorithme pourraient être examinées par une cour. En revanche, si c'est le contenu algébrique et mathématique de l'algorithme qui est visé, des dimensions liées au droit d'auteur ne peuvent être éludées. Les algorithmes, au même titre que les idées et les concepts, ne peuvent *a priori* faire l'objet d'une appropriation sous forme de droit d'auteur ou de brevet [327]. Par contre, si un

323 Sur ce phénomène de substitution, voir D. MOCKLE, « Politiques, directives et instruments de gestion », préc., note 55, par. 18.01-18.3 (« Solutions de rechange à la réglementation »).

324 J.-B. AUBY, préc., note 266, p. 844.

325 P. ISSALYS et D. LEMIEUX, préc., note 276, chap. 8, p. 715.

326 Terrence J. SEJNOWSKI, *The Deep Learning Revolution*, Cambridge (MA), Londres, MIT Press, 2018, chap. 12, p. 171 et suiv.

327 En vertu du par. 27(8) de la *Loi sur les brevets*, L.R.C. 1985, c. P-4, « Il ne peut être octroyé de brevet pour de simples principes scientifiques ou conceptions théoriques ». Selon l'Office de la propriété intellectuelle du Canada (OPIC), il n'est pas possible de faire breveter un principe scientifique, une conception théorique, une idée (..) ou un programme d'ordinateur; OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA (OPIC), *Le guide des brevets*, en ligne : https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/fra/h_wr03652.html#whatYouCanPatent1.

ou plusieurs algorithmes sont intégrés dans un logiciel pour effectuer des opérations de sélection et de classement, les dimensions de droit d'auteur ne sont plus du même type, car ce sont alors des droits de propriété intellectuelle sur un programme informatique[328]. Cette forme d'opacité s'ajoute à l'opacité technique qui résulte de leur utilisation. Pour notre part, nous estimons que le rôle effectif des administrations publiques sera sans doute déterminant. Elles ne seront vraisemblablement pas à l'origine des logiciels de traitement dont elles vont se prévaloir mais, pour les modalités de leur utilisation, le principe de transparence devrait prévaloir.

Afin de remédier à ces problèmes d'accès, les autorités fédérales privilégient depuis 2009 l'utilisation de « normes ouvertes et de logiciels libres à source ouverte »[329]. À des fins de transparence, la *Directive sur la prise de décision automatisée* impose à l'autorité responsable de l'utilisation d'un système décisionnel automatisé de « déterminer la licence appropriée pour les composants logiciels » dans le but d'offrir des sources ouvertes. À défaut de pouvoir utiliser des logiciels libres, les autorités fédérales cherchent à se prévaloir d'un droit d'accès pour l'utilisation d'une «licence propriétaire»[330]. Mais dans la mesure où cette volonté d'accéder aux composants d'un logiciel est énoncée par voie de directive et non par

---

328 David VAVER, *Intellectual Property Law: Copyright, Patents, Trade-Marks*, 2e éd., Toronto, Irwin Law, 2011, p. 70 et suiv. (« Computer Programs »). Cet auteur précise néanmoins ceci (p. 71) : « The program's concepts and ideas, however, have no copyright. » Si l'OPIC considère qu'un code informatique, en tant que tel, n'est pas un bien matériel et ne constitue pas une invention brevetable en vertu de la loi, un programme informatique qui apporte une solution nouvelle peut l'être; OPIC, *Le guide des brevets*, préc., note 327.

329 Secrétariat du Conseil du trésor du Canada, *Directive sur la gestion des technologies de l'information*, Ottawa, 2009, C.2.3.8 , en ligne (à titre d'archive, car cette directive a été abrogée en 2020) : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=15249 .

330 « Si l'on utilise une licence propriétaire, veiller à ce que le gouvernement du Canada détienne le droit d'accéder au système décisionnel automatisé et d'effectuer des essais sur celui-ci (..) si de telles actions sont nécessaires pour réaliser un audit, une enquête, une inspection, un examen, une mesure d'exécution ou une procédure judiciaire, sous réserve de garanties contre une divulgation non autorisée »; *Directive sur la prise de décision automatisée*, préc., note 7, art. 6.2.5.2.

une disposition législative qui aurait pu être conciliée plus facilement avec des dimensions de propriété intellectuelle, chaque ministère et organisme devra s'assurer d'obtenir cet accès lors du contrat d'approvisionnement. À défaut de garantie offerte par la législation, l'outil contractuel offre plus de possibilité.

Dans une perspective de contrôle judiciaire, il est nécessaire de faire la distinction entre la production de documents et le témoignage des agents de l'État. Aux fins de l'application de l'article 46 (1) de la *Loi sur les Cours fédérales*[331], la définition du terme « document » inclut des « données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable[332] ». Le cas échéant, un privilège de non-divulgation peut être revendiqué par « un affidavit de documents[333] ». Afin de déterminer si un document électronique est admissible en preuve, « tout usage ou toute pratique » qui se rattache à la manière de l'enregistrer ou de le mettre en mémoire peut être pris en considération, eu égard, notamment, « à la nature et à l'objet du document[334] ». Selon la *Loi sur la preuve*, l'expression « document électronique » est définie de la même façon qu'en ce qui concerne le fonctionnement des cours fédérales, car ce type de document correspond à un ou plusieurs dispositifs qui « contiennent des programmes d'ordinateur ou d'autres données[335] ». Sur ce plan, la comparaison avec la législation québécoise offre d'autres perspectives, la notion de document y ayant été précisée de manière à inclure les logiciels[336]. Enfin, la divulgation de renseignements reste sujette à des possibilités d'opposition fondées sur des raisons d'intérêt public (le secret administratif) dont la pertinence peut être appréciée par la Cour fédérale ou une cour supérieure[337].

331 *Loi sur les Cours fédéral*es, L.R.C. 1985, c. F-7, art. 46 (1) al. ii.

332 *Règles des Cours fédérales*, DORS/98-106, art. 222 (1).

333 *Id*., art. 223 (2).

334 *Loi sur la preuve au Canada*, L.R.C. 1985, c. C-5, art. 31.5.

335 *Id*., art. 31.8.

336 *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, art. 71. Cette loi doit être lue avec quelques dispositions du *Code civil du Québec* relatives aux moyens de preuve, notamment les articles 2855 et 2860 (force probante et document technologique, respectivement).

337 *Loi sur la preuve*, préc., note 334, art. 37 (1) et (3); art. 283 C.p.c.

Pour ce qui est des considérations relatives aux dimensions contentieuses, il ne faut pas perdre de vue la distinction entre le contentieux administratif et le contentieux constitutionnel. Aux fins de notre analyse sur les algorithmes, le contentieux administratif permet de mettre en lumière des dimensions relatives au principe de légalité, notamment le respect des exigences de la loi, les conditions d'exercice du pouvoir discrétionnaire, ainsi que les exigences de l'équité procédurale. Le contentieux constitutionnel offre la possibilité de réintroduire l'une des questions les plus controversées relativement à l'utilisation des algorithmes, soit celle de la discrimination induite par leur usage[338]. Dans la perspective de l'application des garanties offertes par la *Charte canadienne des droits et libertés*[339], le recours à des algorithmes constitue une forme de l'action gouvernementale[340].

338 Tout en reconnaissant que les algorithmes peuvent engendrer de la discrimination, un auteur suggère de recentrer l'analyse sur l'encadrement des données, et non sur la configuration des algorithmes : Ignacio N. COFONE, « Algorithmic Discrimination Is an Information Problem », (2019) 70-6 *Hastings Law Journal* 1389, 1416 (« Focus on Data Regulation, Not Algorithmic Regulation »). Pour des publications orientées vers la justice pénale, voir en droit américain : Sonja B. STARR, « Evidence-based Sentencing and the Scientific Rationalization of Discrimination », (2014) 66-4 *Stanford Law Review* 803, 836 (« The Social Harm of Demographic and Socioeconomic Sentencing Discrimination »); Sandra G. MAYSON, « Bias in, Bias out », (2019) 128-8 *Yale Law Journal* 2218, 2227 (« The Impossibility of Race Neutrality »). Pour une étude du contexte canadien, voir Kate ROBERTSON, Cynthia KHOO et Yolanda SONG, *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*, Toronto, Faculté de droit, Citizen Lab et International Human Rights Program, 2020.

339 *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982* [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)], art. 32.

340 Ce constat a été fait en droit américain : Kate CRAWFORD et Jason SCHULTZ, « AI Systems as State Actors », (2019) 119 *Columbia Law Review* 1941, 1944 (« Seeing like a State AI System »). La jurisprudence de la Cour suprême du Canada sur la portée de l'article 32 de la *Charte canadienne des droits et libertés*, préc., note 305, rend cette assimilation vraisemblable si l'organisme est une « entité gouvernementale ». Si un algorithme est utilisé pour l'exécution d'un programme gouvernemental, la nature de l'entité n'est pas le seul élément à prendre en considération.

C) La perspective de la justice prédictive

Notre analyse a privilégié l'utilisation des algorithmes par des administrations publiques « classiques » qui exercent des fonctions administratives pour l'attribution d'autorisations, de prestations ou d'indemnités. L'utilisation des algorithmes par la justice administrative et judiciaire ouvre d'autres perspectives. Ce phénomène est plus vaste que l'utilisation potentielle que peuvent en faire différentes catégories de cours et de tribunaux puisque des acteurs privés de type « jeune pousse » (*start-up*), spécialisés dans les dispositifs juridiques (*legaltechs*), offrent des logiciels d'anticipation aux professionnels du droit et aux compagnies d'assurances dans le but de prévoir les décisions des juges[341]. Notre réflexion se limitera ici au recours à des outils de justice prédictive par les juges et le personnel qui leur est attaché.

Dans un passé rapproché, la perspective d'une justice prédictive avait suscité beaucoup de scepticisme à cause de l'importance des concepts flous en droit et des contraintes inhérentes à l'argumentation[342]. De nombreux travaux peuvent être cités pour la spécificité du raisonnement juridique, spécialement dans le monde de la common law[343]. *A priori*,

341 Quelques acteurs ont acquis une certaine notoriété. À titre d'exemple, pour le droit américain : Lex Machina (LexisNexis) et Watson/Ross (IBM); pour le droit britannique : Luminance et Hart; pour le droit français : Case Law Analytics, Predictive et JurisData Analytics (LexisNexis).

342 Andrée LAJOIE, Régine ROBIN et Armelle CHITRIT, « L'apport de la rhétorique et de la linguistique à l'interprétation des concepts flous », dans Danièle BOURCIER et Pierre MACKAY (dir.), *Lire le droit. Langue, texte, cognition*, Paris, L.G.D.J., 1992, 155; Sébastien MCEVOY, « La question de l'arrêt : le cas de l'argumentation dans le droit », dans Danièle BOURCIER et Pierre MACKAY (dir.), préc., 173.

343 Herbert HART, *The Concept of Law*, 3e éd., Oxford, New York, Oxford University Press, 2012, p. 124 (« The Open Texture of Law »)[1re éd. : 1961]; Martin P. GOLDING, *Legal Reasoning*, New York, A. Knopf, 1984, p. 35 et suiv. (« Types of Legal Argument »); Ronald DWORKIN, *L'empire du droit*, Paris, Presses universitaires de France, 1994, chap. 2, p. 49 (« Concepts d'interprétation ») [*Law's Empire*, 1re éd. : 1986]; Joseph RAZ, *Between Authority and Interpretation: On the Theory of Law and Practical Reason*, Oxford, Oxford University Press, 2009, chap. 8 (« Reasoning with Rules »); Frederick SCHAUER, *Penser en juriste. Nouvelle introduction au raisonnement juridique,* Paris, Dalloz,

plusieurs domaines du droit requièrent une marge d'appréciation et d'interprétation qui n'est pas réductible à des éléments de logique formelle qui iraient dans le sens de l'automaticité.

En dépit de ces réelles contraintes inhérentes au droit, la perspective d'une justice prédictive fondée sur des algorithmes d'anticipation[344] retient désormais l'attention, tant en monde francophone[345] que dans le monde anglophone[346]. Avant cette étape qui peut paraître encore éloignée, la dématérialisation de la justice est déjà une réalité avec l'ambition britannique des tribunaux en ligne (*online courts)* qui a démarré en 2015 pour les affaires civiles de moindre importance[347], ainsi que pour la justice

2018 [*Thinking like a Lawyer: A New Introduction to Legal Reasoning,* 1re éd. : 2009]. Pour le monde francophone, dans la perspective des travaux instaurés par Charles Perelman, voir Stefan GOLTZBERG, *L'argumentation juridique*, 4e éd., Paris, Dalloz, 2019, chap. 2, p. 28.

344 Sur l'analyse prédictive, voir Daniel D. GUTIERREZ, « Guide Inside BIGDATA de l'analyse prédictive », en ligne : < https://www.celge.fr/wp-content/uploads/2015/12/guide-analyse-prédictive.pdf >.

345 Yannick MENECEUR, « Quel avenir pour la justice prédictive? Enjeux et limites des algorithmes d'anticipation des décisions de justice », *La Semaine juridique édition générale,* nº 7, 12 février 2018; Lêmy GODEFROY, « La performativité de la justice prédictive : un pharmakon? », dans St. PRÉVOST et E. ROYER, préc., note 267, 96; Bruno DONDERO, « Justice prédictive : la fin de l'aléa judiciaire? », *Recueil Dalloz*, 2017, p. 532; Thomas CASSUTO, « La justice à l'épreuve de sa prédictibilité », dans St. PRÉVOST et E. ROYER, préc., note 267, 107; Pierre-Luc DÉZIEL, « L'utilisation de renseignements personnels dans le contexte de la justice prédictive : le cas des outils actuariels d'évaluation des risques de récidive », (2018) 60 *Archives de philosophie du droit* 253. Benoît PLESSIX, « Vers une justice administrative prédictive? », dans ASSOCIATION FRANÇAISE POUR LA RECHERCHE EN DROIT ADMINISTRATIF, *Le droit administratif au défi du numérique*, Paris, Dalloz, 2019, 81, à la p. 96 (La justice administrative peut-elle devenir entièrement prédictive?).

346 Ashley DEEKS, « The Judicial Demand for Explainable Artificial Intelligence», (2019) 119-7 *Columbia Law Review* 1829; Catherine MATACIC, « Are Algorithms Good Judges? », (2018) 359 *Science* 263; Andrea L. ROTH, « Trial by Machine », (2016) 104-5 *Georgetown Law Journal* 1245, 1252 (« The Uneven, Contingent Rise of Mechanized Criminal Adjudication »).

347 Nick HOLMES, « The Online Court and the Digitisation of Justice», *Infolaw Newsletter*, juin 2019, en ligne : < infolaw.co.uk >. Cette réforme de la justice fait suite au dépôt du rapport du groupe de travail dirigé par le professeur Richard

administrative en France avec l'application Télérecours, lancée en 2012[348] et devenue obligatoire depuis le 1er janvier 2017[349]. Le Québec a élaboré des plans afin d'assurer la transition numérique de la justice pour 2023[350]. Pour ce qui est du reste du Canada, il faut reconnaître le rôle avant-gardiste de la Colombie-Britannique qui a créé en 2012 le British Columbia Civil Resolution Tribunal, fort probablement le premier exemple de justice offerte en ligne[351].

Comme en témoignent ces exemples, la dématérialisation ne serait que la première étape d'une évolution technologique en plusieurs temps, l'usage plus ou moins exhaustif de l'algorithme ne venant qu'en dernier, dans des matières qui se prêtent à ce type de calcul pour des décisions automatisées[352]. La première étape, très contemporaine, celle de la cyberjustice, retient davantage l'attention compte tenu des difficultés liées au fait d'assurer la présence des parties et de leurs avocats dans le contexte

SUSSKIND, *Online Dispute Resolution for Low Value Civil Claims*, février 2015, en ligne : < https://www.judiciary.uk/publications/online-dispute-resolution-for-low-value-civil-claims-2/ >.

348 *Décret nº 2012-1437 du 21 décembre 2012 relatif à la communication électronique devant le Conseil d'État, les cours administratives d'appel et les tribunaux administratifs*, JORF nº 0299 du 23 décembre 2012.

349 Laurence HELMLINGER, « Télérecours : la dématérialisation devient obligatoire devant les juridictions administratives pour les avocats et les administrations », (2017) 1 *RFDA* 12.

350 « Mettre la Justice à l'heure des nouvelles technologies,», dans GOUVERNEMENT DU QUÉBEC, *Le plan pour moderniser le système de justice au Québec : pour une Justice plus innovante et plus efficiente, au bénéfice de tous*, Québec, 2018, en ligne : < https://www.justice.gouv.qc.ca/ministere/dossiers/transformation/ >; MINISTÈRE DE LA JUSTICE DU QUÉBEC, *Plan stratégique 2019-2023*, Québec, 2019, p. 22, en ligne : < https://www.quebec.ca/gouv/ministere/justice/publications/plan-strategique-mjq-2019-2023/ >.

351 BRITISH COLUMBIA CIVIL RESOLUTION TRIBUNAL, en ligne : < https://civilresolutionbc.ca >. Ce tribunal a été créé par la *Civil Resolution Tribunal Act*, S.B.C. 2012, c. 25.

352 Cette analyse chronologique a été proposée par Marc CLÉMENT, « Algorithmes au service du juge administratif : peut-on en rester maître? », (2017) 43 *AJDA* 2453, 2454.

de la pandémie de COVID-19[353]. Si les travaux de Richard Susskind ont connu un regain d'intérêt en raison du contexte pandémique[354], cette situation confère surtout une acuité particulière au virage numérique de la justice[355]. Ainsi, au Québec, le Tribunal administratif du travail et le TAQ ont amorcé un virage numérique qui devrait être achevé en 2021[356].

Cette évolution de la justice dépasse les limites de notre analyse centrée sur la mutation numérique des administrations publiques. Toutefois, ces dimensions revêtent une grande importance pour l'évolution de la justice administrative au Canada. Cette dernière correspond en partie, et non de façon exclusive, à un contentieux technique où les éléments de quantification et de mesurabilité s'avèrent déterminants pour l'appréciation des faits (logement, indemnités, prestations). Ce contentieux technique équivaut, dans une perspective relativement similaire, à ce qui a été décrit comme des « conflits de basse intensité[357] ». Les tribunaux administratifs disposent déjà de bases de données considérables, ne serait-ce que pour permettre l'emploi de termes de recherche afin d'analyser leurs décisions

353 Le Laboratoire de cyberjustice de l'Université de Montréal a élaboré une plateforme de règlement en ligne (PARLe) afin d'offrir une solution de rechange au ralentissement des activités judiciaires : en ligne : < https://nouvelles.umontreal.ca/article/2020/04/03/la-cyberjustice-en-temps-de-pandemie/ >.

354 Richard SUSSKIND, *Online Courts and the Future of Justice*, Oxford, Oxford University Press, 2019, p. 95 et suiv.

355 Ethan KATSH et Orna RABINOVICH-EINY, *Digital Justice. Technology and the Internet of Disputes*, New York, Oxford University Press, 2017; Karim BENYEKHLEF et Jie ZHU, « À l'intersection de l'ODR et de l'intelligence artificielle : La justice traditionnelle à la croisée des chemins », (2020) 25-3 *Lex Electronica* 34, 61 (La dématérialisation de la justice : une tendance irréversible).

356 Pour le TAQ, le dépôt d'un recours en ligne est consultable uniquement dans le cas de la Section des affaires sociales : en ligne : < https://riil.servicestaq.gouv.qc.ca/taq.riil.presentation/ >. Dans le cas du Tribunal administratif du travail, ce service est offert pour la Division de la santé et de la sécurité du travail ainsi que pour la Division de la construction et de la qualification professionnelle : en ligne : < https://www.tat.gouv.qc.ca/menu-utilitaire/services-en-ligne >.

357 Cette expression est employée afin de désigner des litiges (consommation, logement, services publics, travail, infractions pénales mineures) où les questions de droit restent peu complexes : Karim BENYEKHLEF et Jie ZHU, « Intelligence artificielle et justice : justice prédictive, conflits de basse intensité et données massives », (2018) 30-3 *Les Cahiers de propriété intellectuelle* 789, 796.

antérieures. À cet égard, les outils numériques ne peuvent que faciliter la synthèse de leur jurisprudence par rapport à des éléments factuels qui se prêtent à la quantification. L'usage de logiciels de systématisation aux fins de synthèse algorithmique paraît donc inéluctable, notamment dans le domaine de l'indemnisation. Ainsi, en 2017 le Laboratoire de cyberjustice a proposé la mise au point d'un modèle prédictif à partir des décisions rendues antérieurement par la Régie du logement[358].

La prudence est cependant indispensable, car il ne faut pas déduire de cette évolution que tout sera automatisé en matière de justice administrative car, pour établir un taux d'incapacité par exemple, un examen médical reste requis. Ce ne serait ou sera qu'une fois ce taux déterminé, que le juge administratif pourrait ou pourra évaluer, au même titre qu'un décideur administratif, le montant admissible par la synthèse des éléments du dossier, particulièrement sur la base de ce qui a déjà été attribué dans des cas à peu près identiques. En ce qui concerne l'avenir de la profession juridique, c'est une autre dimension à l'égard de laquelle il ne faut pas être trop pessimiste[359], malgré les projections proposées par Susskind[360]. Comme le montrent plusieurs décisions rendues par les tribunaux administratifs, l'appréciation de certains types de faits en matière d'attribution de permis ne se prête pas à une évaluation algorithmique. Le retrait d'un permis d'alcool pour cause d'atteinte à la tranquillité publique en est un exemple, car le tribunal est alors appelé à évaluer la crédibilité d'un ou de plusieurs témoignages, sans oublier le comportement des parties. Il est néanmoins possible de prévoir l'usage des algorithmes au sein des tribunaux administratifs dans certaines matières. De façon prudente et réaliste, il serait utile de mener quelques expériences pilotes afin d'offrir

358 Le logiciel JusticeBot offre les services d'un agent conversationnel qui permet de prévoir le type de décision qui pourrait être rendue en matière de logement locatif : en ligne : < https://www.cyberjustice.ca/projets/justicebot/ >.

359 Brian SIMPSON, « Algorithms or Advocacy: Does the Legal Profession Have a Future in a Digital World? », (2016) 25 *Information & Communications Technology Law*, 50 (la réponse à la question posée dans le titre de cet article sera positive si la formation des juristes est revue en conséquence de ces changements).

360 Richard SUSSKIND, *The End of Lawyers? Rethinking the Nature of Legal Services*, New York, Oxford University Press, 2008, p. 99 et 217.

aux justiciables, sur une base volontaire, la possibilité de se prévaloir d'un logiciel d'anticipation pour le résultat de leur demande. Au même titre que la conciliation, la justice prédictive pourrait compléter les mécanismes de rechange déjà offerts. Le tribunal, avec l'accord des parties, pourrait entériner le résultat et l'inclure dans ses décisions. Au Québec, les cours et les tribunaux ont l'habitude de recourir à des projets pilotes. Ce type de précaution donnerait au législateur le recul nécessaire afin de modifier la loi en vue de déterminer des balises[361].

Pour les justiciables, le caractère volontaire de cette démarche se révèle essentiel. La « maîtrise par l'utilisateur[362] » a été reconnu à titre de principe général dans la *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires* de 2018, au même titre que quatre autres principes : 1) le respect des droits fondamentaux; 2) l'absence de discrimination; 3) la qualité et la sécurité; et 4) la transparence, la neutralité et l'intégrité[363]. Cette charte confirme la nécessité de reconnaître des garanties analogues à celles que nous avons mises en évidence en matière de procédure administrative non contentieuse. La transparence technique en est un exemple, car un système algorithmique « pourrait être également explicable dans un langage clair et vulgarisé afin de décrire la manière dont il produit ses résultats, en communiquant par exemple sur la nature des prestations proposées, les outils développés, les performances et les risques d'erreur[364] ». Il est aussi nécessaire d'éviter une automatisation complète, qui serait dépourvue de toute appréciation qualitative. L'utilisation des algorithmes peut susciter des craintes légitimes à ce sujet. Sur ce point, la Charte affirme que « le professionnel de la justice » (en fait, ce sont surtout les juges et leurs auxiliaires) doit conserver,

---

361 Dans le cas de la *Loi sur la justice administrative*, préc., note 287, il faudrait ajouter quelques dispositions après la section IV du chapitre VI relative à la conciliation (art. 119.6-124).

362 Cette expression inclut les professionnels de la justice.

363 COMMISSION EUROPÉENNE POUR L'EFFICACITÉ DE LA JUSTICE, *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement*, 2018, p. 7, en ligne : < https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b > (ci-après « Charte éthique européenne »).

364 *Id*., p. 11.

à tout moment, la possibilité de ne plus utiliser un système automatisé « au vu des spécificités d'une affaire concrète[365] ». La Charte offre en annexe une étude menée par un groupe d'experts scientifiques sur le recours à l'intelligence artificielle par les systèmes judiciaires des États membres du Conseil de l'Europe[366]. Elle offre une mine de renseignements pertinents pour le fonctionnement de la justice au Canada.

Enfin, parmi diverses pistes d'analyse, on ne peut que s'interroger sur le contenu du RGPD pour l'évolution future du droit canadien. Bien qu'il ne s'applique pas directement au Canada[367], il offre une base utile de comparaison. Sur le plan des principes, il interdit l'automatisation complète et exhaustive des décisions individuelles[368], sous réserve de trois exceptions, notamment si le droit de l'Union européenne ou celui d'un État membre « prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée[369] ». L'exclusion de l'automatisation complète était déjà acquise dans certains droits nationaux au sein de l'Union européenne, comme le montre l'exemple de la France depuis 1978. Le RGPD n'offre pas *a priori* de distinction entre les décisions issues d'une fonction administrative par opposition à celles qui découlent d'une fonction juridictionnelle. Le véritable enjeu consiste à déterminer si un logiciel de prédiction de décisions administratives ou juridictionnelles correspond à un processus

365 *Id.*, p. 12 : « Le professionnel de la justice devrait à tout moment pouvoir revenir aux décisions et données judiciaires ayant été utilisées pour produire un résultat et continuer à avoir la possibilité de s'en écarter au vu des spécificités de l'affaire concrète. »

366 *Id*., annexe 1 : « Étude approfondie sur l'utilisation de l'IA dans les systèmes judiciaires, notamment les applications d'IA assurant le traitement des décisions et des données judiciaires. »

367 Les entreprises canadiennes présentes dans les États membres de l'Union européenne doivent tout de même respecter le RGPD. Plusieurs avis ont été diffusés sur ce sujet, notamment celui du CONSEIL CANADIEN DES NORMES, en ligne : < https://www.scc.ca/fr/RGPD >.

368 « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » : RGPD, préc., note 25, art. 22 (1).

369 *Id.,* art. 22 (2) b.

d'automatisation complète, ce dont on peut douter, car l'examen des faits requiert plusieurs types d'appréciation où l'expertise des décideurs reste déterminante. Il n'en demeure pas moins probant que ce processus d'automatisation, même partiel, représente un « virage mathématique du droit[370] ».

Conclusion

Si le droit du numérique devait être appréhendé comme un tout, la réponse requise pour le choix des instruments ne pourrait qu'être nuancée. Certains domaines ne se prêtent pas beaucoup, ou fort peu, à des interventions législatives, ce qui explique le recours à des instruments de droit souple. À la fin de leur ouvrage sur l'intelligence artificielle et les robots, Alain Bensoussan et Jérémy Bensoussan offrent une liste qui regroupe une vingtaine de textes sous forme de chartes, de lignes directrices, de principes, de codes d'éthique, de déclarations, de modèles de convention, ainsi que des réflexions et des livres blancs en provenance d'acteurs publics et privés qui disposent d'une réelle expertise dans ce domaine[371]. En dépit de la relative incertitude liée à cet essor technologique, les deux auteurs n'en proposent pas moins une synthèse des enjeux juridiques en regroupant plusieurs types de droit sous trois rubriques : les droits en filiation (parmi lesquels figurent le droit d'accès aux algorithmes, le droit à la compréhension et le droit à l'information), les droits de rupture (qui regroupent la responsabilité et la vigilance) et les droits fondamentaux (où l'on trouve, entre autres, la dignité et l'intimité). Malgré sa généralité, le droit du numérique soulève des enjeux précis qui rejoignent des concepts fondamentaux largement connus des juristes.

---

370 Antoine GARAPON et Jean LASSÈGUE, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, Presses universitaires de France, 2018, p. 104 (nouvelle approche «droit et mathématiques»); Alain SUPIOT, *La Gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Paris, Fayard, 2015, p. 215 et suiv.

371 A. BENSOUSSAN et J. BENSOUSSAN, préc., note 237, p. 451 et suiv. Dans cette perspective, la *Déclaration de Montréal pour le développement responsable de l'intelligence artificielle* (2018) présente un réel intérêt : en ligne : < https://www.declarationmontreal-iaresponsable.com/la-declaration >.

La transition numérique des administrations publiques apparaît ainsi sous un éclairage différent. Elle réactualise une dimension classique du droit public, puisqu'il est alors question des droits et des garanties de la population par rapport à l'action publique et gouvernementale. Depuis les progrès décisifs accomplis aux XIX^e^ et XX^e^ siècles en matière de contentieux administratif et de contentieux constitutionnel, l'action administrative doit répondre à des impératifs largement connus suivant les traditions nationales : le principe de légalité, la primauté du droit (*rule of law*) et l'État de droit. L'utilisation de l'intelligence artificielle et des algorithmes ne peut échapper à ces exigences en matière d'action publique[372], notamment dans le contexte canadien, à des impératifs issus des droits reconnus dans la *Charte canadienne des droits et libertés*[373], ainsi que dans la *Charte des droits et libertés de la personne*[374]. Comme le montre l'état des réflexions outre-Atlantique, le numérique oblige à repenser la question des droits fondamentaux[375]. Le 8 avril 2020, le Conseil de l'Europe a publié des lignes directrices afin d'énoncer des obligations qui incombent aux États à l'égard de la protection et de la promotion des droits de la personne et des libertés fondamentales pour l'utilisation de systèmes algorithmiques[376].

372 Emily BERMAN, « A Government of Laws and not of Machines », (2018) 98 *Boston University Law Review* 1277, 1349 (« Undermining the Rule of Law »); Ronan KENNEDY, « Algorithms and the Rule of Law », (2017) 17-3 *Legal Information Management* 170, 171 (« Public Sector Use and Difficulties »).

373 *Charte canadienne des droits et libertés*, préc., note 339.

374 *Charte des droits et libertés de la personne*, RLRQ, c. C-12.

375 LES RAPPORTS DU CONSEIL D'ÉTAT, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, Paris, La Documentation française, 2014, p. 153 et suiv. (l'ambivalence du numérique impose de repenser la question des droits fondamentaux).

376 CONSEIL DE L'EUROPE, *Recommandation CM/Rec (2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme*, Strasbourg, 8 avril 2020, en ligne : < https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016809e1124 >. À titre de rappel, le Canada occupe une position d'observateur au sein du Conseil de l'Europe depuis 1996 et participe activement à de nombreux comités, notamment celui qui est lié aux enjeux soulevés par l'intelligence artificielle et l'utilisation des algorithmes.

Dans la *Stratégie de transformation numérique gouvernementale*, le Québec énumère six vecteurs d'accélération où la question du droit est absente[377]. Il est possible d'argumenter que la « performance numérique » des administrations publiques requiert des transformations substantielles sur le plan technique[378], ainsi que pour les habilités requises, notamment en matière de culture et de compétence numérique. Afin d'assurer « des relations adaptées à la réalité des citoyens », les autorités ont priorisé l'amélioration technique des services[379], sans tenir compte de l'autre dimension, qui est celle des « droits », mais aussi celle du droit pour lequel il n'y avait pas de stratégie. À l'heure actuelle, le cadre législatif – québécois ou canadien – n'est pas approprié en vue d'offrir des balises[380].

Pour remédier à ce déséquilibre, plusieurs solutions peuvent être étudiées. La première consiste à modifier quelques lois afin de proposer un cadre juridique mieux adapté à cette transition numérique. De nombreux enjeux de la transition numérique rejoignent un corpus de lois préexistantes[381], comme en témoigne la législation en matière de protection de la vie privée et d'accès à l'information. Ce scénario de modification de la législation reste le plus plausible ainsi que le montre le cheminement du projet de loi nº 64 au Québec depuis juin 2020[382]. Au niveau fédéral, la législation dans ce domaine sera peut-être modifiée dans un avenir rapproché[383]. Sur ce point, le Commissaire à la vie privée du Canada

377 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, préc., note 12 : 1) Gouvernance numérique; 2) Culture et compétences numériques; 3) Innovation numérique; 4) Écosystème numérique; 5) Architecture, gestion et sécurité de l'information; 6) Performance numérique.

378 K. MENSAH, préc., note 53.

379 SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, préc., note 12, p. 6.

380 Sur ce point, le constat de l'inadaptation du cadre juridique avait déjà été fait en 2004 par K. BENYEKHLEF, préc., note 106, p. 276.

381 Outre la *Loi sur l'administration publique*, préc., note 57, d'autres lois sont pertinentes, notamment la *Loi concernant le cadre juridique des technologies de l'information*, préc., note 5, et la *Loi sur la justice administrative*, préc., note 287, art. 2-8.

382 Projet de loi nº 64, préc., note 145.

383 JUSTICE CANADA, *Modernisation de la Loi sur la protection des renseignements personnels du Canada*, juin 2020, en ligne : < https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/dd-dp/index.html >.

recommandait en 2019 la modernisation des lois sur la protection des renseignements personnels[384]. Si cette étape s'avère indispensable pour le respect du droit à la vie privée, le deuxième scénario, plus ambitieux, aurait été d'offrir une loi de transition numérique plus exhaustive en matière de droits et libertés, à la lumière des initiatives récentes menées au Québec et en Ontario. Si cette loi de transition peut correspondre, en tout ou en partie, au contenu du RGPD, afin d'offrir des balises plus précises pour les droits des internautes, le droit comparé montre également qu'une loi peut viser de façon plus particulière la transformation numérique des administrations publiques. Enfin, la dernière solution, plutôt axée sur des enjeux de droit administratif, pose des difficultés considérables dans le contexte canadien en l'absence de codification de la procédure administrative non contentieuse.

Dans la recherche de nouvelles solutions, le principe de transparence[385] est appelé à jouer un rôle déterminant. Largement reconnu comme principe de bonne gouvernance et de bon gouvernement[386], il transcende plusieurs types de savoir qui ont pour objet l'étude des administrations publiques et, de façon plus générale, le fonctionnement des organisations[387]. Il figure également dans les nombreuses chartes et déclarations de principe relatives à divers aspects du numérique. Sur ce fondement, les administrations publiques devraient fournir une information minimale sur le type de données personnelles qu'elles recueillent, sur les garanties de confidentialité qu'elles offrent et sur leur utilisation de ces données (le site Web de chaque organisme devrait être mis à contribution). Dans le même esprit, elles devraient indiquer qu'elles se servent d'un ou de plusieurs algorithmes aux fins de processus en partie automatisés, notamment pour en expliquer les modalités d'utilisation. Enfin, pour

384 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2018-2019*, préc., note 227, p. 8 (« Réforme des lois sur la protection des renseignements personnels »).

385 Au Québec, ce principe est explicitement reconnu dans l'article premier de la *Loi sur l'administration publique*, préc., note 57.

386 Daniel MOCKLE, « Le principe général du bon gouvernement », (2019) 60-4 *C. de D*. 1031, 1072.

387 Jens FORSSBAECK et Lars OXELHEIM (dir.), *The Oxford Handbook of Economic and Institutional Transparency*, New York, Oxford University Press, 2015, p. 5.

réactualiser dans un sens plus contemporain les exigences de motivation propres au droit administratif, les autorités administratives devraient mentionner dans leurs décisions le poids réel d'un algorithme afin d'en expliquer les conditions d'utilisation. Si les autorités abordent ces dimensions par voie de politiques et de directives, elles le font en ordre dispersé sans recourir à la législation.

D'autres questions doivent aussi être évaluées par le législateur. Suivant l'exemple offert par le RGPD, faut-il reconnaître le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, en incluant le profilage? Un compromis possible serait de reconnaître cette garantie, sauf si le législateur prévoit expressément un processus complet d'automatisation dans le traitement de données. Dans la mesure où l'identité numérique de chaque citoyen ou citoyenne est appelée à devenir sous peu la normalité, il paraît indispensable de préciser les composantes de cette identité par le recours à la législation. De même, la numérisation de données personnelles en vue de préciser les contours de cette identité ouvre la perspective de l'utilisation de moyens techniques de plus en plus efficaces pour la reconnaissance faciale et la traçabilité de toute la population par l'insertion de dispositifs sur les téléphones intelligents. À tout le moins, les critères de sécurité devraient être définis par la loi. Enfin, la question de l'accessibilité risque d'être récurrente en dépit de l'optimisme affiché par les autorités[388]. Si l'accessibilité est l'un des objectifs de la *Loi sur l'administration publique*[389], l'égalité n'est pas aussi explicite. Afin d'éviter l'exclusion, faut-il réaffirmer l'égalité dans l'accès aux services publics peu importe les garanties offertes par les chartes?

---

388 Outre le facteur générationnel, des dimensions sociales et économiques peuvent induire l'exclusion, notamment pour les personnes peu scolarisées : Serge KABLAN, Arthur OULAÏ et Emma ELLIOTT, « Legal Aspects of Accessibility and Usability of Online Public Services in Quebec and Canada», (2015) 15-3 *Electronic Commerce Research* 387, 396 (distinction proposée entre les termes *accessibility* and *usability*). Ce texte commente également les positions de la Cour fédérale sur le sujet dans l'arrêt *Jodhan* c. *Procureur général du Canada*, 2010 CF 1197. Pour un bilan plus récent dans le contexte de la pandémie de Covid-19 : A. BAHARY-DIONNE et K. GENTELET, préc., note 31, p. 10 (trois dimensions des inégalités numériques).

389 *Loi sur l'administration publique,* préc., note 57, art. 6.

Notre étude ne saurait prétendre à l'exhaustivité dans l'évaluation de ces enjeux[390] : cependant, la dimension centrale n'en reste pas moins celle de la légitimité du droit et de la législation dans la transition numérique des administrations publiques. Sans balises juridiques, le virage numérique annoncé par le Conseil du trésor du Québec, ainsi que par celui du Canada, pourrait n'être qu'une redite de la première transition numérique, celle du « moment 2000 ». Si les événements liés à la pandémie de COVID-19 accélèrent le rythme de la transition numérique et son intensité, il faut souhaiter que le « moment 2020 » puisse refléter un meilleur équilibre dans le choix des instruments d'action. En dépit de leur utilité administrative, les outils de gestion de type lignes directrices, politiques, chartes administratives et stratégies ne peuvent résoudre les vraies questions, celles qui sont liées au droit, mais encore moins celles des droits. Le Québec a désormais amorcé un mouvement favorable à la législation, et le Canada, au niveau fédéral, doit également le faire dans la perspective du droit public. Pour reprendre la formule largement connue de Dworkin qui vise les droits fondamentaux (*taking rights seriously*), il faut prendre le droit plus au sérieux pour la transition numérique des administrations publiques[391].

390 Cette étude est largement orientée vers les relations des administrations publiques avec le public. L'exhaustivité aurait nécessité d'aborder l'automatisation du travail au sein des administrations publiques, notamment pour le travail à distance, ainsi que l'usage de robots et de machines autonomes afin de remplacer des catégories de personnel ou de pallier le vieillissement de la main-d'œuvre.

391 Ronald DWORKIN, *Prendre les droits au sérieux*, Paris, Presses universitaires de France, 1995.