QUELLES ŒILLÈRES IMPOSER À L'ÉTAT ? LE REGARD DU DROIT QUÉBÉCOIS SUR LA TECHNOLOGIE À RECONNAISSANCE FACIALE UTILISÉE PAR LES FORCES DE L'ORDRE AU ROYAUME-UNI

Samy CHEKIR[1]

1

Résumé

Dans cette contribution, nous portons un regard critique sur le recours aux caméras de surveillance munies d'une technologie de reconnaissance faciale par les autorités policières dans les lieux publics. Plus précisément, nous procédons à l'analyse d'une décision rendue par la High Court of Justice au Royaume-Uni ayant rejeté le recours d'un individu qui contestait la légalité de cette nouvelle technique d'enquête. Les arguments étudiés s'inscrivent essentiellement sous deux volets, soit d'une part le droit à la vie privée comme droit fondamental et d'autre part, l'encadrement législatif de ces technologies.

Nous procédons ensuite à l'analyse de la situation sous l'angle du droit canadien et québécois. Au terme de cette brève étude, nous constatons un certain nombre de similitudes entre le droit anglais et le droit canadien et québécois, et ce, tant sur le plan du droit de la vie privé que sur l'encadrement des technologies pouvant lui porter atteinte. Ceci étant, certaines différences nous laissent croire qu'un tribunal canadien n'en serait pas arrivé aux mêmes conclusions que la High Court of Justice dans l'état actuel du droit. Évidemment, la porte demeure ouverte pour le législateur qui peut en tout temps intervenir afin de permettre ou interdire le recours à une telle technologie par les autorités policières.

INTRODUCTION

[1] Les avancés technologiques des dernières années ont permis à certains États d'augmenter la surveillance sur leur territoire[2]. C'est ainsi que les gouvernements se sont de plus en plus dotés de caméras de surveillance leur permettant d'observer les faits et gestes de leurs citoyens. Plus récemment, s'est ajoutée une intelligence capable d'identifier automatiquement les personnes repérées par le biais de la reconnaissance faciale.

[2] Nous entreprendrons ici l'ambitieuse tâche de porter un regard sur les applications possibles de cette technologie et les limites de son utilisation en procédant à l'analyse d'une décision rendue par la High Court of Justice au Royaume-Uni[3]. L'exposé de ce cas d'étude nous permettra d'identifier certaines des nombreuses[4] règles applicables à l'utilisation de cette technologie par les autorités anglaises. Pour ce faire, nous porterons, dans un premier temps, un regard sur les protections offertes aux droits fondamentaux affectés avant de passer, dans un second temps, au cadre normatif structurant le recours à cette technologie. Nous nous attarderons par la suite à une étude analogue de certaines règles applicables au Québec dans un contexte similaire.

I. ROYAUME-UNI

I.1. CONTEXTE

[3] En septembre 2019, la High Court of Justice d'Angleterre et du Pays de Galles rendait une décision[5] portant sur la légalité de l'utilisation de caméras de surveillance à reconnaissance faciale en direct par les forces policières de South Wales (ci-après « SWP »)[6]. Le demandeur, Edward

2 Elly Cosgrove, *One billion surveillance cameras will be watching around the world in 2021, a new study says*, CNBC, 6 décembre 2019, en ligne : https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html; Matthew Keegan, *Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled*, The Guardian, 2 décembre 2019, en ligne : https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled; et Hannah Devlin, *'We are hurtling towards a surveillance state': the rise of facial recognition technology*, The Guardian, 5 octobre 2019, en ligne : https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state.

3 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin) (Demande d'autorisation d'appel accueillie).

4 Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf.

5 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3.

6 Pour une étude complète de l'utilisation de cette technologie par la SWP voir : Bethan Davies, Martin Innes et Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff Universities' Police Science Institute, 2018, en ligne : https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf.

Bridges, soutient être victime, comme bien d'autres, de violations à son droit à la vie privée des suites de l'utilisation par la SWP de l'outil AFR Locate[7]. Plus précisément, le demandeur soulève trois moyens identifiés par la Cour comme étant (1) la violation de son droit à la vie privée garanti par la *Convention européenne des droits de l'homme*[8], (2) la violation de ses droits prévus par les lois sur la protection des renseignements personnels et (3) l'obligation du secteur public de traitement égal des citoyens[9]. La présente étude ne fera état que des deux premiers moyens.

I.2. ANALYSE DE LA DÉCISION

A. *CONVENTION EUROPÉENNE DES DROITS DE L'HOMME*

[4] Se fondant sur l'article 8 de la *Convention* qui consacre le droit à la vie privée et ses limites, le demandeur estime que les nouvelles techniques d'enquête policières portent atteinte à ses droits fondamentaux. Au terme de l'analyse de ce premier moyen, la Cour conclut qu'il est vrai que le traitement de données biométriques des citoyens par les forces de l'ordre constitue une entrave importante à leur droit à la vie privée[10]. Le fait que ce traitement se produise dans un lieu public n'affecte en rien cette conclusion, puisque les citoyens conservent une expectative raisonnable de vie privée à l'égard de leur données biométriques même dans ces lieux[11]. En l'espèce, la Cour se dit toutefois satisfaite que le cadre normatif en place comprenant le *Data Protection Act 2018*[12], dont nous ferons état plus loin, le *Surveillance Camera Code of Practice*[13] ainsi que les politiques mises en place par la SWP suffisent à répondre au critère du second alinéa de l'article 8 de la *Convention*, soit la nécessité que l'ingérence soit

7 Pour une explication, voir Bethan Davies, Martin Innes et Andrew Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, Cardiff Universities' Police Science Institute, 2018, en ligne : https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bdafb4403ce64828d6fbc04/1541077838619/AFR+Report+%5BDigital%5D.pdf, p. 4. Voir également : *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341 (Admin) (Demande d'autorisation d'appel accueillie), par. 7, 23 et suiv.

8 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. no 5 (entrée en vigueur le 3 septembre 1953) (ci-après « *Convention européenne des droits de l'Homme* » ou « *Convention* »).

9 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 18.

10 *Ibid*., par. 59 à 62 ; Voir aussi Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file.

11 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 54 et 57.

12 *Data Protection Act 2018*, 2018 c. 12. Notons, à titre informatif, que cette loi intègre au droit national les principes édictés par le *Règlement général sur la protection des données*, règlement no 2016/679. À cet effet, voir : Department for Digital, Culture, Media & Sport, *Data Protection Act 2018. Factsheet – Overview*, p. 2, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf.

13 Surveillance Camera Commissionner, *Surveillance Camera Code of Practice*, 2014, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

prévue par la loi[14]. Soulignons de plus que l'ingérence doit également constituer « une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »[15]. Ce dernier volet est satisfait dès lors que l'ingérence passe le test établi par la jurisprudence[16], comme en l'espèce[17].

B. LOIS PARTICULIÈRES

[5] En ce qui concerne les revendications sous ce chapitre, nous concentrons notre analyse sur les articles 34 et 35 de la *Data Protection Act 2018* (ci-après « DPA 2018 ») d'une part et sur l'article 64 de cette même loi d'autre part.

[6] Suite à une analyse détaillée de ces dispositions, le Tribunal conclut dans un premier temps que le recours à la technologie AFR Locate est strictement nécessaire à l'accomplissement des fonctions de la SWP[18] et que l'objectif poursuivi est par ailleurs d'intérêt public[19]. La Cour déplore cependant le caractère trop général de la politique mise en place par la SWP pour l'utilisation de AFR Locate, mais elle retient qu'il revient au Commissaire à l'information d'établir les éléments que doivent prévoir de telles politiques. En l'espèce, la politique de la SWP, bien que peu précise en règle générale, suffit au contexte propre de l'affaire. Le Juge n'ira que d'un commentaire suggérant à la SWP de bonifier ses politiques suivant les recommandations du Commissaire à l'information lorsque celles-ci seront disponibles[20]. Avec égard, nous sommes d'avis que la Cour est passée à côté de l'opportunité de statuer sur l'obligation d'adopter une politique détaillée prévoyant certains éléments et abordant certains sujets

14 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 85 à 91 et 96. Ce constat ne fait pas l'unanimité : Jamie Grace, Machine Learning Technologies and Their Inherent Human Rights Issues in Criminal Justice Contexts, 2019, en ligne : https://ssrn.com/abstract=3487454 ou http://dx.doi.org/10.2139/ssrn.3487454.

15 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. no 5 (entrée en vigueur le 3 septembre 1953), art. 8.

16 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, [2019] EWHC 2341, préc., note 3., par. 98 ; Voir aussi : Bank Mellat v Her Majesty's Treasury (No 2) [2014] AC 700, par. 20.

17 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, préc., note 3, par. 99 et s.

18 *Ibid*., par. 137. À ce sujet, voir Information Commissioner, *The use of live facial recognition technology by law enforcement in public places, Information Commissioner's Office*, 2019/01, p. 14 à 16, en ligne : https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

19 *Ibid*.

20 *Ibid*., par. 139 à 141.

nécessaires à la satisfaction de l'objet du DPA 2018. À défaut, nous devons, nous aussi, nous en remettre aux futurs directives et communiqués du Commissaire à l'information afin de mieux saisir la portée de ces politiques.

[7] Dans un second temps, la Cour rappelle qu'en plus de l'adoption de politiques, une autorité policière souhaitant traiter des données du public doit également produire une évaluation de l'impact qu'aura le traitement qu'elle envisage faire sur les données personnelles en question et leur protection, le tout en vertu de l'article 64 DPA 2018[21]. Elle estime que la SWP satisfait ici à cette exigence[22].

[8] À la lumière de ce qui précède, nous retenons que le législateur anglais souhaite responsabiliser les contrôleurs de données face aux enjeux liés à la protection des renseignements personnels. Pour ce faire, il leur impose des obligations en amont du traitement de ces renseignements par l'adoption de politiques internes et en procédant à l'évaluation des risques potentiels. De plus, le traitement des données par un contrôleur est encadré par des principes généraux prévus dans la loi[23] en plus de règles strictes applicables à certaines situations particulières[24].

II. CANADA - QUÉBEC

[9] Dans un esprit comparatif, nous étudierons le recours éventuel à une technologie comparable par les autorités policières canadiennes sous les mêmes angles que ceux précédemment abordés. Nous verrons donc d'abord (II.1.) le droit à la vie privée garanti par la *Charte canadienne des droits et libertés*[25] (ci-après « *Charte canadienne* ») avant de nous intéresser plus particulièrement au (II.2.) régime mis en place par le législateur et applicable au traitement de données biométriques.

---

21 *Data Protection Act 2018*, 2018 c. 12, art. 64. L'évaluation imposée par cet article fait également l'objet d'une suggestion du Commissaire aux caméras de surveillance : Surveillance Camera Commissioner, *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems*, 2019, p. 3 et 4, en ligne : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf. Voir aussi Information Commissioner, *The use of live facial recognition technology by law enforcement in public places, Information Commissioner's Office*, 2019/01, p. 13 et 14, en ligne : https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

22 *Bridges, R (On Application of) v The Chief Constable of South Wales Police*, préc., note 3, par. 148.

23 *Data Protection Act 2018*, 2018 c. 12, art. 35 à 40.

24 *Ibid*., art. 35(3) et (5).

25 *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)].

II.1. *CHARTE CANADIENNE DES DROITS ET LIBERTÉS*

[10] Le droit à la vie privée est consacré par l'article 8 de la *Charte canadienne* qui garantit la protection contre les fouilles, les perquisitions et les saisies abusives[26]. Le recours à la technologie de reconnaissance faciale par les forces policières étant une technique relativement nouvelle, peu de décisions se sont penchées sur la question[27]. Il faut donc selon nous s'en remettre à la jurisprudence concernant le traitement des données biométriques[28] ou, plus largement, la protection de la vie privée informationnelle[29].

[11] Avant toute chose, il faut nous demander si la donnée biométrique constitue un renseignement personnel susceptible de bénéficier de la protection de l'article 8 de la *Charte canadienne*. À ce sujet, que l'on se fie à la définition de la Cour suprême[30], qui fait référence aux caractère intime des détails que révèle un renseignement personnel, ou à celle du législateur[31], qui se fonde plutôt sur le fait qu'un renseignement est personnel dès lors qu'il permet l'identification de l'individu concerné, force est de constater qu'une donnée biométrique doit être considérée comme étant un renseignement personnel. Elle est ainsi susceptible de bénéficier de la protection de l'article 8 de la *Charte canadienne*.

[12] Il importe de préciser que ces données ne sont que susceptibles de bénéficier de cette protection étant donné le champ d'application de l'article 8 qui se limite aux cas où il existe une attente raisonnable de la

---

26 *R.* c. *Mills*, 2019 CSC 22, par. 12; *R.* c. *Reeves*, 2018 CSC 56, par. 2 et 11; *R.* c. *Jones*, 2017 CSC 60, par. 38 ; *R.* c. *Spencer*, 2014 CSC 43, par. 15; *R.* c. *Dyment*, [1988] 2 R.C.S. 417 ; *Hunter* c. *Southam*, [1984] 2 R.C.S. 145. Voir également en doctrine : Karim Benyekhlef et Pierre-Luc Déziel, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Éditions Yvon Blais, 2018, p. 80 et suiv.; Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 3 et Julie M. Gauthier, *Le droit de la biométrie au Québec : sécurité et vie privée*, Montréal, Éditions Yvon Blais, 2015, p. 35.

27 *R.* v. *Voong*, 2018 ONCJ 352, par. 8 et suiv. L'argument du caractère personnel des données biométriques extraites par la technologie à reconnaissance faciale ne fait pas l'objet d'une analyse par la Cour.

28 Dans son mémoire, Julie M. Gauthier suggère que la technologie de reconnaissance faciale traite des données biométriques. Elle discute également des données biométriques de façon plus large comme étant des renseignements personnels. Suivant ce raisonnement ces données tomberaient sous l'égide du droit à la vie privée : Julie M. Gauthier, *Le droit de la biométrie au Québec : sécurité et vie privée*, préc., note 26, aux pages 22, 23 et 27 à 33.

29 La Cour suprême identifie trois sphères dans lesquelles un individu peut bénéficier d'un droit à la vie privée, soit les sphères territoriale, personnelle et informationnelle : *R.* c. *Dyment*, [1988] 2 RCS 417, par. 19. Voir également : Karim Benyekhlef et Pierre-Luc Déziel, *Le droit à la vie privée en droit québécois et canadien*, préc., note 26, aux pages 85 et 86 et Julie M. Gauthier, préc., note 26, 2015, p. 35.

30 *R.* c. *Plant*, [1993] 3 R.C.S. 281, p. 293. L'application de cette notion a par la suite été élargie par la Cour suprême dans *R.* c. *Spencer*, [2014] 2 R.C.S. 212. Voir également : Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 89 et 91.

31 Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21), art. 3 et Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A-2.1, art. 54.

part d'un individu à la protection de ces renseignements[32]. Cette attente raisonnable s'évalue, selon la jurisprudence, sous le couvert de nombreux critères que l'on peut regrouper en quatre catégories, soit « (1) l'objet de la fouille ou de la perquisition contestée; (2) le droit du demandeur à l'égard de l'objet; (3) l'attente subjective du demandeur en matière de respect de sa vie privée relativement à l'objet; et (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances »[33].

[13] En l'espèce, comme mentionné précédemment, le traitement des données biométriques affecte la sphère informationnelle de la vie privée. De plus, ces données étant des renseignements personnels, l'individu visé bénéficie d'un droit à l'égard de celles-ci. De même, considérant la nature de ces données, il est raisonnable de croire qu'un individu visé aurait une attente subjective à l'égard de sa vie privée. Finalement, nous sommes d'avis que les données biométriques du visage permettant l'identification en temps réel d'une personne relèvent de son cœur biographique et, pour cette raison, justifient une attente objectivement raisonnable en matière de respect à la vie privée[34]. Il faut donc conclure que le traitement de ce type de données constitue une fouille et une saisie au sens de l'article 8 de la *Charte canadienne*. Reste à savoir si cette fouille et saisie est abusive.

[14] Le caractère abusif d'une fouille ou d'une saisie se présumera si celles-ci ne sont pas expressément autorisées[35]. Il faudra, pour renverser cette présomption, établir que la fouille, la saisie ou la perquisition est permise par une règle de droit, que celle-ci est raisonnable et que la fouille, la perquisition ou la saisie s'est réalisée raisonnablement[36]. En l'espèce, c'est la common law qui, selon nous, constituerait la règle de droit permettant la fouille ou la saisie, puisqu'elle confère, aux policiers canadiens, des pouvoirs similaires à ceux des policiers anglais[37]. Par ailleurs, le caractère raisonnable de la règle de droit est établi dans la

32 Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 87 et 89. Voir également : *R.* c. *Spencer*, [2014] 2 R.C.S. 212, par. 16 et Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 3.

33 *R.* c. *Spencer*, [2014] 2 R.C.S. 212, par. 18. Voir également : *R.* c. *Mills*, 2019 CSC 22, par. 13; *R.* c. *Reeves*, 2018 CSC 56, par. 28; *R.* c. *Jones*, 2017 CSC 60, par. 13; Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, aux pages 93 et 94 ; Gerald Chan et Nader R. Hasan, *Digital Privacy Criminal, Civil and Regulatory Litigation*, Toronto, LexisNexis Canada, 2018, p. 5.

34 *R.* c. *Cole*, [2012] 3 R.C.S. 34. Cité par Karim Benyekhlef et Pierre-Luc Déziel, préc., note 26, 94. Voir également les facteurs énumérés par la Cour suprême dans l'évaluation de la quatrième catégorie de facteurs dans *R.* c. *Tessling*, [2004] 3 R.C.S. 432, par. 32. Cité par I*bid*., p. 97.

35 *Hunter* c. *Southam*, [1984] 2 R.C.S. 145, p. 160 et 161. Cité par *Ibid*., p. 102. L'autorisation pourra notamment prendre la forme d'un mandat.

36 *Ibid*., p. 103. Voir aussi *R.* c. *Collins*, [1987] 1 R.C.S. 265.

37 Martin Vauclair et Tristan Desjardins, *Traité général de preuve et de procédure pénales*, 26e éd., Montréal, Éditions Yvon Blais, 2019, par. 212 et suiv., p. 95 et s.

mesure où il existe « un juste équilibre entre l'atteinte à la vie privée qu'elle suppose et l'importance ou la valeur de l'objectif sociétal qu'elle poursuit »[38]. Finalement, l'analyse du caractère raisonnable de l'exécution de la fouille, la perquisition ou la saisie se fera au cas par cas considérant la nature hautement factuelle de ce dernier critère.

[15] En ce qui concerne le recours aux technologies de reconnaissance faciale par les corps policiers, nous avons de la difficulté à croire qu'une règle de droit permettant une telle mesure soit considérée comme raisonnable. En effet, le traitement aléatoire des données biométriques du visage de tous les passants d'un lieu public sans motif particulier relatif à chacun d'entre eux semble faire fi de l'importance de la balance entre l'objectif poursuivi et le droit à la vie privée des individus concernés[39]. Malgré notre doute, et suivant les similitudes entre les cadres d'analyse anglais et canadiens, il est tout à fait possible qu'un tribunal canadien, aux prises avec la même question, en arrive à une conclusion similaire[40].

[16] Ceci étant, la jurisprudence et la doctrine insistent, tout comme l'a fait la jurisprudence anglaise[41], sur la nécessité d'un encadrement des mesures de surveillance technologiques auxquelles ont recours les forces policières[42]. Ainsi, l'utilisation de la technologie de reconnaissance faciale se doit d'être balisée si elle doit passer le test de la jurisprudence.

II.2. LOIS PARTICULIÈRES

[17] Il est désormais acquis que les données biométriques traitées par les technologies de reconnaissance faciale sont des renseignements personnels au sens des lois québécoise et canadienne[43]. Ainsi, notre étude de ces lois se fera sous l'angle des dispositions prévoyant des obligations similaires à celles prévues au DPA 2018 vues précédemment.

38 K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 109.

39 Ce n'est d'ailleurs pas pour rien que des dispositions spécifiques visant l'octroi d'un mandat général permettant d'avoir recours à des dispositifs de surveillance électronique existent au *Code criminel* tels que l'art. 487.01(4) et (5). Même dans le cadre de l'émission de ce type de mandat, l'article 487.01(1) C.cr. prévoit notamment que les forces policières doivent détenir des motifs suffisants justifiant l'émission du mandat.

40 Bien que, par le passé, la Cour suprême ait mis en garde les autorités contre l'utilisation de technologies de surveillance vidéo des citoyens : *R.* c. *Wong*, [1990] 3 R.C.S. 36. Voir l'analyse qu'en fait la doctrine dans K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 239.

41 *Supra*, note 13. Voir également *S v. United Kingdom*, (2009) 48 EHRR 50, par. 99 et 103.

42 K. Benyekhlef et P.-L. Déziel, préc., note 26, aux pages 239 à 243. Voir également : *R.* c. *Wong*, [1990] 3 R.C.S. 36 et *R.* c. *Duarte*, [1990] 1 R.C.S. 30.

43 Soit respectivement la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 et la *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.

[18] La loi québécoise prévoit que la collecte des données par un organisme public doit être « nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion »[44]. N'étant pas sans rappeler les dispositions anglaises vues précédemment[45], cet article a été interprété comme établissant une obligation de stricte nécessité[46]. Ce critère ne semble pas trouver son pendant du côté fédéral, bien que le législateur ait tout de même choisi de limiter la collecte des renseignements personnels à « ceux qui ont un lien direct avec ses programmes ou ses activités »[47]. En dépit de cette différence et à défaut d'une définition de l'expression « lien direct »[48], nous sommes d'avis que les renseignements personnels collectés par une institution fédérale doivent également respecter un critère de nécessité[49]. Toutefois, bien qu'exigé par la loi anglaise, le critère d'intérêt public que doit revêtir le traitement des données semble absent des lois québécoise et canadienne les rendant plus souples à cet égard, distinction qu'il importe de souligner.

[19] De plus, notons l'absence non seulement de l'obligation d'adopter des politiques relatives à la protection des renseignements personnels[50], mais également de l'obligation de procéder à une évaluation du risque inhérent à la collecte et au traitement de ces renseignements. L'absence de ces obligations nous paraît regrettable, puisqu'elles permettraient de mieux conscientiser les organismes visés et d'assurer une réflexion de leur part en amont de la collecte et de l'utilisation des données recueillies. Cette

---

44 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 64 al. 2. La loi québécoise est plus stricte, à cet égard, que le DPA 2018 en ce qu'elle ne fait pas de distinction entre données sensibles ou non, tout renseignement personnel devant satisfaire au critère de nécessité.

45 Les dispositions québécoises et canadiennes semblent regrouper, en une seule disposition pour chaque loi, les obligations imposées par les paragraphes 35(1)a) et 35(1)b) DPA 2018.

46 *Syndicat des employées et employés professionnels et de bureau, section locale 57* et *Caisse populaire St-Stanislas de Montréal*, 1998 QCSAT 2765 et *M.L.* c. *Gatineau (Ville de)*, 2010 QCCAI 68. Cité par K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 318. Voir également : Julie M. Gauthier, préc., note 26, p. 70 et suiv.

47 *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, art. 4.

48 K. Benyekhlef et P.-L. Déziel, préc., note 26, p. 273.

49 *Ibid*., p. 319 ; Voir également : Commissariat à la protection de la vie privée du Canada, Reconnaissance faciale automatisée dans les secteurs public et privé, Gatineau, 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/, p. 8 et 9. Une telle interprétation est, selon nous, conforme à l'esprit de la loi qui vise la protection des renseignements personnels de la population.

50 Quoique le Commissariat à la protection de la vie privée du Canada recommande l'adoption de politiques : Commissariat à la protection de la vie privée du Canada, Reconnaissance faciale automatisée dans les secteurs public et privé, Gatineau, 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/, p. 9.

absence milite selon nous en faveur d'un moratoire[51] sur le recours à la technologie de reconnaissance faciale par les autorités policières dans l'attente d'un encadrement législatif mieux adapté à cette nouvelle réalité. À tout événement, ceci ne signifie pas que les lois québécoise et canadienne fournissent aux citoyens une protection plus faible, puisqu'à titre d'exemple, la loi québécoise édicte tout de même une obligation de « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels [...] »[52].

[20] Notons en dernier lieu que le législateur québécois a prévu des dispositions au sujet de l'utilisation de données biométriques[53]. L'article 44 LCCJTI prévoit à cet effet que « [n]ul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques »[54]. Nous n'avons retracé aucune décision ayant interprété cette disposition[55]. Cependant, il semblerait qu'à sa lecture même, l'article 44 LCCJTI constitue un obstacle imposant au recours à la technologie qui nous occupe[56].

CONCLUSION

[21] À la lumière de la présente étude, nous constatons que le droit à la vie privée en tant que droit fondamental est protégé de manière similaire au Royaume-Uni et au Canada. Toutefois, ceci ne signifie pas pour autant que les cadres d'analyse développés par les tribunaux anglais et canadiens seront appliqués de la même manière. Leur application peut être influencée par bien des facteurs, que ce soit les valeurs de ces sociétés qui, à certains égards, peuvent diverger, ou encore le corpus législatif concernant la protection des renseignements personnels qui peut orienter l'analyse des décideurs dans un sens comme dans l'autre. À

51 Cette approche est adoptée ailleurs dans le monde, notamment en Australie ainsi que dans certaines villes américaines telles que San Francisco et Seattle : Kate Crawford, Roel Dobbe, Theodora Dryer, Genevieve Fried, Ben Green, Elizabeth Kaziunas, Amba Kak, Varoon Mathur, Erin McElroy, Andrea Nill Sánchez, Deborah Raji, Joy Lisi Rankin, Rashida Richardson, Jason Schultz, Sarah Myers West, and Meredith Whittaker. *AI Now 2019 Report*, New York, AI Now Institute, 2019, p. 32, en ligne : https://ainowinstitute.org/AI_Now_2019_Report.html.

52 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, art. 63.1.

53 *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1, art. 44 et 45 (ci-après « LCCJTI »).

54 *Ibid*., art. 44.

55 À l'exception d'une décision rendue par la Commission d'accès à l'information par laquelle elle rejette l'argument suivant lequel une empreinte vocale constitue une donnée biométrique : *C.R.* c. *Loto-Québec*, 2012 QCCAI 300.

56 Sous réserve d'une intervention législative similaire à celle se trouvant à la *Loi sur le système correctionnel du Québec*, RLRQ c S-40.1, qui à son article 18.0.1 écarte expressément l'application de l'article 44 LCCJTI.

cet effet, bien que certaines des obligations imposées au contrôleur de données par la loi anglaise le sont également aux organismes publics par les lois fédérale et québécoise, ces règles présentent certaines distinctions.

[22] Pour finir, ce texte ne se veut pas un plaidoyer à l'encontre de l'instauration, au Canada, d'une technologie comme celle utilisée par le service de police de South Wales. Les autorités policières devraient bénéficier des innovations technologiques afin de demeurer à jour dans la poursuite de leur mission. Cela dit, il faut selon nous éviter de verser systématiquement dans le « technosolutionnsime ». En ce sens, on ne peut tolérer qu'il ne soit porté atteinte de façon déraisonnable et arbitraire aux droits fondamentaux des citoyens au nom du combat contre la criminalité.