« Habeas data» en droit canadien

par

Pierre Trudel, France Abran et Jie Zhu

Chaire L.R.Wilson sur le droit des technologies de l'information et du commerce électronique

Centre de recherche en droit public

Faculté de droit

Université de Montréal

2013

Table des matières

Le contexte 2

1. Règles générales de protection des données personnelles 3
   - 1.1 Description générale du régime juridique et esprit du système de protection canadien 4
   - 1.2 Caractéristiques des données protégées 6
     - 1.2.1 Aux termes des différentes lois sur la protection des renseignements personnels 6
     - 1.2.2 Selon les lois sur la protection des droits de la personne 7
     - 1.2.3 Le droit à la vie privée garanti par le droit commun privé provincial 8
     - 1.2.4 Les atteintes à la vie privée sanctionnées par le droit criminel canadien 10
   - 1.3 Encadrement du traitement des données 10
     - 1.3.1 Formalités préalables à un traitement de données 10
     - 1.3.2 Droits des personnes visées par le traitement 11
     - 1.3.3 Élaboration de statistiques s'appuyant sur des données personnelles 11
   - 1.4 Autorités de contrôle 12
     - 1.4.1 Les organismes de surveillance administrative 12
     - 1.4.2 Le rôle des autorités judiciaires dans la protection des renseignements personnels 13

2. Protection de la personne lors de traitements de données personnelles à des fins administratives ou judiciaires 13
2.1 Protection lors de traitement de données intéressant la sûreté de l'État ou de données relatives aux infractions criminelles 14
2.1.1 Divulgation de renseignements intéressant la sûreté de l'État 14
2.1.2 Gestion des dossiers criminels 14
3.1 Protection de données biométriques 16
3.1.1 Prélèvement de données biométriques chez les accusés 16
3.2.2 Dans le cadre du programme canadien d'immigration et de protection des réfugiés 20
3.3.3 Autres mesures provinciales relativement au traitement des données biométriques 21

Bilan et perspective 21

Le contexte

Le Canada est doté d'une structure fédérale, le droit applicable en matière de données personnelles découle aussi bien des règles de droit provinciales que des règles fédérales. Les préoccupations au sujet de la protection des renseignements personnels ont vu le jour au Canada avec l'avènement des ordinateurs, qui ont augmenté les risques de porter massivement atteinte à la vie privée, vers la fin des années 1960 et le début des années 1970[1]. En partant des mêmes constats, l'Organisation de coopération et de développement économique (OCDE) a cherché à harmoniser les pratiques relatives à la protection des données des pays membres en établissant des normes minimales pour le traitement des renseignements personnels, d'où l'adoption, en 1980, des *Lignes directrices régissant la protection de la vie privée et les flux transfrontalières de données de caractère personnel*.

Le Canada a adhéré à ces lignes directrices en 1984. À l'époque, les lois canadiennes n'encadraient que l'action des gouvernements et des organismes gouvernementaux. En 1996, l'Association canadienne de normalisation (CSA) publie le *Code type sur la protection des renseignements personnels*, document qui, s'inspirant des lignes directrices de l'OCDE, consacre dix (10) principes de la protection de la vie privée dans les secteurs public et privé. Approuvés par le Conseil canadien des normes, ils abordent deux (2) sujets d'inquiétudes : d'une part, la façon dont les organisations collectent, utilisent, communiquent et protègent les renseignements personnels; d'autre part, le droit des individus d'avoir accès aux renseignements personnels les concernant et de les faire corriger, le cas échéant :

1) **Responsabilité** : une organisation est responsable de l'information personnelle en sa possession et doit nommer une ou plusieurs personnes imputables pour la conformité de l'organisation avec les principes qui s'appliquent.

---

[1] Pour un historique sur la question, voir : Nancy HOLMES, *Les lois fédérales du Canada sur la protection de la vie privée*, Parlement du Canada (Division du droit et du gouvernement), le 25 septembre 2008, en ligne : <http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0744-f.htm#note2>.

2) **Détermination des fins de la collecte** : le but pour lequel l'information personnelle est collectée doit être identifié par l'organisation au moment ou avant de recevoir cette information.

3) **Consentement** : la connaissance et le consentement de l'individu sont nécessaires pour obtenir, utiliser ou divulguer l'information personnelle sauf dans les cas appropriés.

4) **Limitation de la collecte** : la collecte de l'information personnelle doit être limitée à ce qui est nécessaire pour le but identifié par l'organisation. L'information sera collectée selon des moyens justes et légaux.

5) **Limitation de l'utilisation, de la communication et de la conservation** : l'information personnelle ne doit pas être utilisée ni divulguée pour des fins autres que celles pour laquelle elle a été fournie sauf avec le consentement de l'individu ou selon les exigences de la loi. L'information personnelle doit être conservée seulement le temps nécessaire pour satisfaire les buts visés.

6) **Exactitude** : l'information personnelle doit être précise, complète et à jour en conformité avec les buts visés.

7) **Mesures de sécurité (sauvegardes)** : l'information personnelle doit être protégée par des sauvegardes de sécurité appropriées à la nature critique de l'information.

8) **Transparence (ouverture)** : une organisation doit pouvoir fournir promptement aux individus l'information spécifique sur ses politiques et pratiques en rapport avec la gestion de l'information personnelle.

9) **Accès aux renseignements personnels (accès individuel)** : sur demande, un individu doit être informé de l'existence, de l'utilisation et de la divulgation de ses informations personnelles et doit pouvoir obtenir cette information. Un individu doit pouvoir questionner la précision et l'état complet de cette information et la faire modifier au besoin.

10) **Possibilité de porter plainte à l'égard du non-respect des principes** : un individu doit pouvoir questionner la conformité en fonction des principes précités auprès des individus responsables de la conformité dans l'organisation.

Avec certaines modifications mineures, ce code volontaire sera intégré à la *Loi sur la protection des renseignements personnels et les documents électroniques*[2]. Du coup il deviendra obligatoire pour les entreprises assujetties à cette législation fédérale.

Mais afin de compléter cette mise en contexte, il convient de décrire le cadre général de la protection des données personnelles en droit canadien.

1. Règles générales de protection des données personnelles

Au Canada, la protection des renseignements personnels est une compétence partagée. Elle est régie à la fois par des lois provinciales et fédérales, au Québec, ces matières relèvent du droit civil d'inspiration française, tandis que dans les autres provinces, c'est la common law telle que reçue dans ces territoires qui trouve application. Des mécanismes constitutionnels et des mesures quasi constitutionnelles procurent certains éléments du cadre juridique applicable à l'*Habeas Data*.

---

[2] L.C. 2000, ch. 5, art. 5.

1.1 Description générale du régime juridique et esprit du système de protection canadien

Au niveau constitutionnel, la *Charte canadienne des droits et libertés*, entrée en vigueur le 17 avril 1982, enchâsse le droit de chacun « à la vie, à la liberté et à la sécurité de sa personne » (art. 7) ainsi qu'« à la protection contre les fouilles, les perquisitions ou les saisies abusives » (art. 8). Bien que le respect de la vie privée n'y soit pas spécifiquement affirmé, les tribunaux ont interprété ces articles comme comportant une garantie contre les intrusions déraisonnables dans la vie privée par la puissance publique[3], surtout en matière criminelle[4].

Au Canada, les lois sur la protection des droits et libertés fondamentaux de la personne jouissent d'un statut dit « quasi constitutionnel », en ce qu'elles orientent l'interprétation des autres lois à moins d'une dérogation expresse à l'intérieur d'une loi en particulier. Quoique la plupart de ces textes[5] ne prévoient pas un droit spécifique à la vie privée, ces lois peuvent néanmoins être invoquées dans des situations où des discriminations peuvent exister et nuire incidemment à la vie privée, notamment en matière d'égalité en milieu de travail[6].

Au sein du fédéralisme canadien, le droit commun est en principe de compétence provinciale[7]. Au Québec, sous l'ancien *Code civil du Bas Canada*, la protection de la vie privée était assurée par une interprétation prétorienne de la notion de faute civile, soit tout écart de conduite (intentionnel ou non) qui s'éloigne de celle qu'aurait adoptée un « bon père de famille » (*cf.* art. 1053 C.c.B.C.). Depuis 1994, le nouveau Code civil contient des dispositions garantissant spécifiquement le respect de la vie privée et de la réputation[8], sans pour autant évacuer les notions de faute (évaluée désormais sous l'angle d'une personne raisonnable), de dommage et de lien de causalité comme éléments déclencheurs de la responsabilité civile (art. 1457 C.c.Q.) en matière d'atteinte à la vie privée. Dans les autres provinces et les territoires, la common law traditionnelle n'a pas caractérisé la violation de la vie privée comme constitutive d'un délit civil (« *tort* ») spécifique[9]. Certaines provinces[10] ont néanmoins consacré le « *right of privacy* » dans

---

3 *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(1) : « La présente charte s'applique : au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest; à la législature et au gouvernement de chaque province, pour tous les domaines relevant de cette législature. » Y compris les corps municipaux : *Godbout* c. *Longueuil (Ville)*, [1997] 3 R.C.S. 844.

4 *Infra*, p. 14.

5 À l'exception de la *Charte des droits et libertés de la personne du Québec* (L.R.Q., c. C-12), voir son article 5 : « Toute personne a droit au respect de sa vie privée. » La violation de ce droit peut donner lieu à une condamnation pour dommages punitifs en cas d'atteinte illicite et intentionnelle (art. 49 al. 2), et ce, indépendamment de la commission d'une faute civile : *de Montigny* c. *Brossard (Succession)*, [2010] 3 R.C.S. 64, par. 44.

6 *Infra*, p. 6.

7 *Loi constitutionnelle de 1867*, 30 & 31 Vict., c. 3 (R.-U.), art. 92 : « Dans chaque province la législature pourra exclusivement faire des lois relatives aux matières tombant dans les catégories de sujets ci-dessous énumérés, savoir : […] 13. La propriété et les droits civils dans la province; ».

8 Il s'agit des articles, 3, 35 et suiv. du *Code civil du Québec*, L.Q. 1991, c. 64, entré en vigueur le 1er janvier 1994.

9 La protection de la vie privée pouvait cependant être assurée indirectement par d'autres remèdes tels que « trespass », « defamation and breach of confidence » ou « injurious falsehood ».

leur législation, pour lequel une action en justice peut être introduite sans qu'il soit nécessaire de prouver un dommage, pourvu que l'atteinte ait été intentionnelle. De son côté, la Cour d'appel de l'Ontario a reconnu explicitement, en janvier 2012, le délit civil de « *privacy tort of intrusion upon seclusion* »[11], apprécié au point de vue d'une personne raisonnable et requérant un élément intentionnel de la part de l'auteur de l'atteinte.

À côté de ces régimes réparateurs du droit commun, la protection de la vie privée, au niveau fédéral comme dans les différentes provinces, est assurée essentiellement par deux (2) lois particulières s'appliquant l'une au secteur public et l'autre, au secteur privé. Au fédéral, il s'agit, d'une part, de la *Loi sur la protection des renseignements personnels*[12] – s'appliquant aux entités du gouvernement fédéral ainsi que des organismes du secteur privé sous contrat avec le gouvernement fédéral – et, d'autre part, de la *Loi sur la protection des renseignements personnels et les documents électroniques*[13] – s'appliquant aux entités du secteur privé dans le cadre d'activités commerciales. La conformité à ces législations est assurée par le Commissariat à la protection de la vie privée du Canada, autorité indépendante qui répond directement à la Chambre des Communes et au Sénat. À ce titre, le commissaire est habilité à enquêter sur les plaintes, à mener des vérifications et à intenter des poursuites judiciaires en vertu des deux (2) lois fédérales. Les décisions du commissaire sont assujetties au contrôle judiciaire de la Cour fédérale, dont la décision peut être portée en appel devant la Cour d'appel fédérale et, en dernier ressort, à la Cour suprême du Canada. Le commissaire est également appelé à effectuer des recherches sur des enjeux liés à la protection de la vie privée de même qu'à sensibiliser la population à cette problématique. Ce modèle[14] est dupliqué au sein de chacune des dix (10) provinces canadiennes et des trois (3) territoires : deux (2) lois principales qui s'appliquent distinctement l'une au secteur public[15] et l'autre, au secteur privé[16]; un organisme de surveillance indépendant qui relève directement de la législature provinciale; contrôle judiciaire exercé par les cours supérieures provinciales. Il est à noter que la plupart de

---

10 Il s'agit des provinces de la Saskatchewan (Privacy Act, R.S.S. 1978, c. P-24), du Manitoba (*Loi sur la protection de la vie privée*, C.P.L.M. c. P125), de la Colombie-Britannique (Privacy Act, R.S.B.C. 1996, c. 373) et de la Terre-Neuve-et-Labrador (Privacy Act, R.S.N.L. 1990, c. P-22).

11 *Jones* v. *Tsige*, 2012 ONCA 32, par. 70 : « One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person ».

12 *Loi sur la protection des renseignements personnels*, L.C. 1980-81-82-83, c. 111 (L.R.C. 1985, c. P-21).

13 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

14 Sous réserve des dispositions particulières dans le domaine des services de santé et des services sociaux, des archives, des dossiers d'adoption, etc.

15 Les provinces de la Saskatchewan, de l'Ontario et de la Nouvelle-Écosse comportent des dispositions statutaires spécifiques applicables aux corps municipaux : *Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1 [Saskatchewan] ; *Loi sur l'accès à l'information municipal et la protection de la vie privée*, L.R.O. 1990, c. M.56 [Ontario] ; *Municipal Government Act*, S.N.S. 1998, c. 18, Part XX [Nouvelle-Écosse]. De plus, la Nouvelle-Écosse régit spécifiquement la communication des renseignements personnels des Néo-Écossais à l'extérieur du Canada par un organisme public provincial : *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3 [Nouvelle-Écosse].

16 La *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, c. 5) [fédéral] s'applique aux organisations privées non assujetties à des lois provinciales ou territoriales essentiellement similaires pour leurs activités intraprovinciales ou intraterritoriales. À ce jour, des décrets d'exclusion ont été émis par le gouverneur en conseil au profit des provinces qui ont adopté leurs propres mesures législatives, à savoir le Québec, la Colombie-Britannique, l'Alberta, l'Ontario, le Nouveau-Brunswick et la Terre-Neuve-et-Labrador. Voir : *Processus de détermination du caractère « essentiellement similaire » d'une loi provinciale par la gouverneure en conseil*, (2002) 136 Gaz. Can. I.

ces lois sur la protection des renseignements personnels[17] sont élevées au rang de mesures quasi constitutionnelles, en ce qu'elles prévalent d'office, en cas d'incompatibilité et à moins de dérogations explicites, sur toute autre mesure législative. Dans tous les cas, le contrôle s'exerce au niveau de la collecte, de l'utilisation, de la communication, de la conservation et du retrait des renseignements personnels.

De plus, une loi fédérale d'application générale, le *Code criminel*[18] prohibe toute interception volontaire d'une communication, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre (art. 184 C.cr.), ainsi que toute utilisation ou divulgation volontaire d'une communication privée ainsi interceptée (art. 193 C.cr.), au risque d'encourir une peine d'emprisonnement.

1.2 Caractéristiques des données protégées

Quel est alors le spectre de données protégées par la notion du respect de la vie privée en droit canadien? Nous évoquerons successivement l'information protégée aux termes des différentes lois – fédérales et provinciales – sur la protection des renseignements personnels (i), les motifs de discrimination interdits selon les législations sur la protection des droits de la personne (ii), le concept de la vie privée garantie par le droit commun privé provincial (iii) ainsi que les comportements prohibés en droit criminel (iv).

1.2.1 Aux termes des différentes lois sur la protection des renseignements personnels

Il y a d'abord les renseignements personnels définis comme tout renseignement – quels que soient sa forme ou son support – qui concerne une personne physique identifiable. Sont compris sous ce chef, outre les coordonnées de la personne[19] et sa correspondance privée ou confidentielle adressée à une institution ainsi que les réponses que celle-ci adresse en retour et qui risquent vraisemblablement de révéler le contenu de la correspondance originale :

- des données biométriques comme le groupe sanguin, les empreintes digitales et des traits héréditaires;
- les antécédents médicaux, criminels, scolaires ou professionnels;
- les avis de cotisations fiscales et les relevés de transactions financières;

---

17 À l'exception de la Colombie-Britannique, de la Nouvelle-Écosse et de la Saskatchewan.

18 *Code criminel*, L.R.C. 1985, c. C-46 ; le droit criminel (sauf la constitution des tribunaux de juridiction criminelle, mais y compris la procédure en matière criminelle) est de compétence fédérale : *Loi constitutionnelle de 1867*, 30 & 31 Vict., c. 3 (R.-U.), art. 91(27).

19 Le nom d'une personne n'est pas nécessairement protégé par toutes les lois fédérales ou provinciales sur la protection des renseignements personnels, à moins qu'il ne soit mentionné avec d'autres données protégées ou encore si la seule divulgation du nom révélerait d'autres renseignements au sujet de la personne : voir *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21, art. 3(*i*) [fédéral]; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, art. 56 [Québec]; *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, c. F.31, art. 2(1)*h*) [Ontario]; *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, art. 24(1)*k*) [Saskatchewan]. Il est à noter que les coordonnées de la personne (« *contact information* ») ne sont pas des renseignements protégées en Colombie-Britannique : *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, schedule 1 « *personal information* » [secteur public] et *Personal Information Protection Act*, S.B.C. 2003, c. 63, art. 1 « *personal information* » [secteur privé].

- certaines données sensibles telles que la race, l'origine nationale ou ethnique, la couleur, l'ascendance, la religion, l'âge, le sexe, l'orientation sexuelle, l'état matrimonial ou familial, les convictions politiques, les opinions personnelles (sauf si elles se rapportent à un autre particulier), voire les opinions d'autrui sur la personne; et
- le numéro d'assurance sociale (NAS) ainsi que tout autre symbole ou signe individuel qui est attribué à la personne.

L'énumération varie d'une loi à l'autre, mais n'est qu'indicative dans tous les cas[20].

1.2.2 Selon les lois sur la protection des droits de la personne

Les lois sur la protection des droits de la personne au Canada, tant au niveau fédéral que provincial, garantissent le droit à l'égalité de tous les Canadiens en prohibant toute discrimination exercée tant par des personnes privées que par les gouvernements et basée sur des motifs précis qui sont limitativement énumérés dans différentes lois. Sous réserve de certaines variantes, il peut s'agir de la race, de la couleur, de l'origine ethnique ou nationale, de la religion ou des croyances religieuses, du sexe (y compris les caractéristiques associées telle la grossesse), de l'orientation sexuelle, de l'état matrimonial, de l'âge – sauf dans la mesure prévue dans la loi, des convictions politiques, du handicap, de la condition sociale, des sources de revenu et des antécédents judiciaires, etc.

Si les lois sur la protection de la personne, à l'exception de la Charte québécoise[21], ne reconnaissent pas explicitement le droit à la vie privée, elles protègent accessoirement certains renseignements personnels pour garantir un accès équitable à l'emploi[22] en interdisant à tout employeur de requérir[23] – par quelque moyen que ce soit – d'une personne de l'information relative aux motifs de discrimination énumérés, sauf s'il s'agit des exigences professionnelles justifiées et, moins fréquemment, dans le cas d'un organisme sans but lucratif à caractère

---

20 Certaines lois prévoient par ailleurs des exclusions expresses : voir *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, c. F.31, art. 2(2) et (3) [Ontario]; *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, art. 24(2) [Saskatchewan]; en Colombie-Britannique, les coordonnées de la personne sont spécifiquement exclues (voir *supra*) de même que, dans le secteur privé, l' « information sur le produit du travail » (« *work product information* ») : *Personal Information Protection Act*, S.B.C. 2003, c. 63, art. 1 « *personal information* ».

21 *Supra*, note 4.

22 La province de la Colombie-Britannique et le territoire du Yukon ne prévoient pas une telle garantie : voir *Human Rights Code*, R.S.B.C. 1996, c. 210 [Colombie-Britannique]; *Loi sur les droits de la personne*, L.R.Y. 2002, c. 116 [Yukon].

23 En Nouvelle-Écosse et à l'Île-du-Prince-Édouard, il est même interdit à l'employeur de simplement « inviter » un postulant à fournir de tels renseignements : voir *Human Rights Act*, R.S.N.S. 1989, c. 214, art. 8(2) [Nouvelle-Écosse] ; *Human Rights Act*, R.S.P.E.I. 1988, c. H-12, art. 6(3) [Île-du-Prince-Édouard].

charitable, philanthropique, religieux, politique ou éducatif[24], voire pour l'application des mesures de discrimination positive[25].

1.2.3 Le droit à la vie privée garanti par le droit commun privé provincial

Au Québec, l'article 36 C.c.Q. liste des exemples non exhaustifs d'actes qui peuvent être considérés comme des atteintes à la vie privée d'une personne, à savoir :

- le fait de pénétrer chez elle ou y prendre quoi que ce soit;
- le fait d'intercepter ou d'utiliser volontairement une communication privée;
- le fait de surveiller sa vie privée par quelque moyen que ce soit;
- le fait de capter ou d'utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
- le fait d'utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public; ainsi que
- le fait d'utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

Cette liste rejoint peu s'en faut les exemples d'atteintes à la vie privée énumérés dans les législations des provinces de common law ayant reconnu statutairement le « *right of privacy* »[26]. De leur côté, les lois sur la protection de la vie privée de la Colombie-Britannique et de la Terre-Neuve-et-Labrador définissent la vie privée en fonction du standard de l'attente raisonnable en prévoyant la nécessité de pondérer toutes les circonstances pour apprécier l'étendue de la protection dont un individu peut raisonnablement s'attendre dans une situation donnée[27].

La collecte, la détention et la communication de renseignements personnels par une personne privée est soumise à aucune autorisation préalable. La jurisprudence québécoise reconnaît le droit pour une entreprise de mettre en place des mécanismes de surveillance dans des circonstances où une personne raisonnable le trouverait approprié et lorsque les moyens utilisés sont raisonnablement justifiables et délimités.

Les tribunaux québécois ont considéré qu'il est permis d'effectuer des activités de surveillance dans la mesure ou celles-ci sont raisonnables et procèdent de motifs légitimes. Dans la décision Bridgestone/Firestone[28], la Cour d'appel du Québec a indiqué qu'il doit y avoir un lien entre la

---

[24] Voir *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 18.1 et 20 [Québec] ; *Code des droits de la personne*, L.R.O. 1990, c. H.19, art. 23(2) et 24(1)*a*) [Ontario] ; *Saskatchewan Human Rights Code*, S.S. 1979, c. S-24.1 [Saskatchewan] ; *Human Rights Act*, R.S.N.S. 1989, c. 214, art. 8(2) et 6*c*)(ii) [Nouvelle-Écosse] ; *Human Rights Act*, R.S.P.E.I. 1988, c. H-12, art. 6(3) et (4)*c*) [Île-du-Prince-Édouard].

[25] Voir *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 18.1 *in fine* [Québec] ; *Loi sur les droits de la personne*, L.Nun. 2003, c. 12, art. 10(1) [Nunavut] ; *Loi sur les droits de la personne*, L.T.N.-O., 2002, c. 18, art. 8(1) [Territoires du Nord-Ouest].

[26] Voir à titre indicatif : *Privacy Act*, R.S.S. 1978, c. P-24, art. 3 [Saskatchewan]; *Loi sur la protection de la vie privée*, C.P.L.M. c. P125, art. 3 [Manitoba].

[27] *Privacy Act*, R.S.B.C. 1996, c. 373 [Colombie-Britannique]; *Privacy Act*, R.S.N.L. 1990, c. P-22, art. 3(2) [Terre-Neuve-et-Labrador].

[28] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (csn)* c. *Trudeau*, 1999 CanLII 13295 (QC C.A.)

mesure de surveillance et l'atteinte des résultats ou objectifs visés par l'entreprise. La Cour d'appel a confirmé de plus l'exigence de motifs rationnels préalables à la démarche et la nécessité d'y procéder par des moyens raisonnables. La Cour d'appel a expliqué à cet égard que :

> [B]ien qu'elle comporte une atteinte apparente au droit à la vie privée, la surveillance à l'extérieur de l'établissement peut être admise si elle est justifiée par des motifs rationnels et conduite par des moyens raisonnables, comme l'exige l'article 9.1 de la Charte québécoise. Ainsi, il faut d'abord que l'on retrouve un lien entre la mesure de surveillance et les exigences du bon fonctionnement de l'entreprise ou de l'établissement en cause. Il ne saurait s'agir d'une décision purement arbitraire et appliquée au hasard. L'entreprise doit déjà posséder des motifs raisonnables avant de décider de soumettre son salarié ou une autre personne à une surveillance. Il ne saurait les créer a posteriori, après avoir effectué la surveillance en litige.

Par conséquent, la surveillance est licite à la condition qu'elle repose sur des motifs sérieux. Il importe par conséquent d'être en mesure de démontrer la légitimité de la surveillance, compte tenu de la situation spécifique de l'entreprise. L'objectif visé par la surveillance doit être clairement identifié et il doit être sérieux et important et viser à régler un problème identifié ou à prévenir un péril identifiable. La surveillance peut viser toute personne. Le fait que des règles spécifiques s'appliquent aux personnes de moins de 18 ans traduits devant les tribunaux ne change rien au droit de surveiller des lieux privés.

Étant donné ces exigences, il faut que les entreprises se dotent des informations permettant, éventuellement de démontrer la survenance des problèmes concrets et réels que l'on veut prévenir ou auxquels on souhaite remédier au moyen des traitements d'informations personnelles. Dans cet esprit, les tribunaux et les arbitres du travail ont reconnu que l'installation de caméras de surveillance est acceptable lorsqu'il est nécessaire de prévenir les vols ou le vandalisme, lorsqu'il y a un réel problème dans l'entreprise ou si le public a accès aux lieux[29] pour protéger un secret industriel[30], pour des motifs de sécurité[31] ou, encore, pour satisfaire à des exigences qui s'imposent à l'entreprise, notamment au regard de la protection d'informations ou des biens. Il est même possible de considérer, comme on l'a fait dans au moins une décision judiciaire, que dès lors qu'ils en sont informés, les personnes visées par les systèmes de surveillance installés dans des lieux généralement accessibles au public ne peuvent invoquer leur droit à la vie privée[32].

Au niveau du choix des moyens, il faut que la mesure de surveillance apparaisse comme nécessaire pour la vérification du comportement des personnes surveillées et que, par ailleurs, elle soit menée de la façon la moins intrusive possible. Lorsque ces conditions sont réunies,

---

29 *Syndicat des travailleuses et travailleurs de la Fabrique Notre-Dame — CSN et Fabrique de la Paroisse Notre-Dame*, D.T.E. 2006T-56; *Ontario (Liquor Control Board of Ontario) and O.L.B.E.U. (Goncalves)*, (2005) 137 L.A.C. (4th) 350; *Canada Safeway Ltd. and U.F.C.W.*, Loc. 401 (Owre) (Re), (2006) 152 L.A.C. (4th) 161; *Janes Family Foods and U.F.C.W.,* Loc. 100A (Re), (2006) 156 L.A.C. (4th) 304; *Re Fraser Surrey Docks Ltd. and International Longshore and Warehouse Union*, Local 514, (2006) 159 L.AC. (4th) 72.

30 *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, D.T.E. 2001T-620.

31 *Gouvernement du Québec (Sécurité publique) et Syndicat des agents de la paix en services correctionnels du Québec*, 2010 CanLII 59735.

32 *Gouvernement du Québec (Sécurité publique) et Syndicat des agents de la paix en services correctionnels du Québec*, 2010 CanLII 59735, EYB 2010-184829, par. 187.

une entreprise a le droit de recourir à des procédés de surveillance, qui doivent être aussi limités que possible. Car les tribunaux ont maintes fois rappelé qu'il doit exister une proportionnalité entre le recours au moyen de surveillance et les périls auxquels on entend remédier.

La surveillance doit être faite de manière proportionnée par rapport aux enjeux. Il faut de même limiter les mesures qui porteraient atteinte à la dignité des personnes comme la surveillance de lieux associés à l'intimité comme les salles de toilettes. De ces exigences, l'on peut inférer que les entreprises doivent s'assurer que leurs mesures de surveillance sont proportionnées, compte tenu des enjeux. Elles doivent également informer les personnes se trouvant dans les lieux surveillés du fait qu'ils sont l'objet de la surveillance de même que de la possibilité que des informations recueillies sont susceptibles d'être partagées.

1.2.4 Les atteintes à la vie privée sanctionnées par le droit criminel canadien

La partie VI du *Code criminel* intitulée « Atteintes à la vie privée » (art. 183 et suiv.) encadre les situations où il serait permis, avec ou sans l'autorisation du juge, d'intercepter une communication privée ainsi que l'admissibilité en preuve de son contenu. Dans les grandes lignes, une interception ne constituera pas une atteinte à la vie privée lorsque l'auteur ou le destinataire de la communication privée y a consenti de façon expresse ou tacite (art. 184(2)*a*) C.cr.). De son côté, un agent de l'État peut effectuer une interception préventive lorsqu'il a des motifs raisonnables de croire qu'il existe un risque de lésions corporelles pour la personne qui a consenti à l'interception ou que celle-ci vise à empêcher les lésions corporelles (art. 184.1 C.cr.), voire dans une situation d'urgence (art. 184.4 C.cr.). Des exceptions sont également pourvues pour les fournisseurs de services téléphoniques, les préposés de Sa Majesté chargés de la régulation du spectre des fréquences de radiocommunication ou les gestionnaires d'ordinateur (art. 184(2)*c*)-*e*) C.cr.). Dans les autres cas, une autorisation judiciaire est requise pour intercepter une communication privée.

1.3 Encadrement du traitement des données

Les règles sur la protection des données personnelles sont formulées en fonction des étapes de leur cycle de vie soit la cueillette, l'utilisation, la communication, la conservation et la destruction des renseignements personnels. Nous aborderons à tour de rôle les formalités préalables à respecter par les organismes responsables (i), les droits des personnes visées (ii), puis l'élaboration de statistiques s'appuyant sur ces renseignements (iii).

1.3.1 Formalités préalables à un traitement de données

Au-delà de la pluralité des lois fédérales, provinciales et territoriales sur la protection des données personnelles au Canada, les obligations auxquelles sont astreintes les responsables partagent *grosso modo* le tronc commun suivant. À l'étape de la collecte, les institutions sont tenues de ne recueillir en principe les renseignements personnels qu'auprès de l'individu lui-même et d'informer ce dernier des fins auxquelles les renseignements recueillis sont destinés. Les renseignements ainsi recueillis ne peuvent être communiqués ou utilisés qu'aux fins auxquelles ils ont été collectés ou avec le consentement de l'individu concerné, à moins que la

loi ne prévoie autrement[33] et sous réserve des cas où le refus de communiquer est rendu obligatoire[34] ou discrétionnaire de par la loi[35]. Au stade de la conservation, les institutions responsables doivent veiller, dans la mesure du possible, à ce que les renseignements personnels utilisés soient à jour, exacts et complets. Le retrait ou la destruction des renseignements personnels est comparativement moins réglementé, sinon qu'ils doivent être conservés pendant une période suffisamment longue pour permettre à l'individu d'exercer son droit d'accès. Les lois provinciales et territoriales, à l'exception de l'Ontario et de la Saskatchewan, obligent également les organismes responsables à prendre des mesures de sécurité raisonnables aux fins de protéger les données recueillies contre des risques d'accès, de collecte, d'utilisation, de communication et de destruction non autorisés, voire de pertes accidentelles.

1.3.2 Droits des personnes visées par le traitement

En contrepartie, les individus concernés par les renseignements personnels traités bénéficient de certains droits corrélatifs, à savoir :

- le droit d'être informés des fins auxquelles les renseignements personnels recueillis sont destinés;
- le droit de refuser de communiquer les renseignements personnels qui les concernent;
- le droit d'accès, *i.e.* de se faire communiquer sur demande – conformément aux procédures prévues dans les différentes lois – les renseignements personnels les concernant; ainsi que
- le droit de rectifier, c'est-à-dire de demander, le cas échéant, la correction ou la destruction des renseignements personnels le concernant qui seraient erronés ou incomplets.

1.3.3 Élaboration de statistiques s'appuyant sur des données personnelles

Aux fins d'élaboration de statistiques, la communication des renseignements personnels *a priori* protégée est autorisée sans le consentement de l'individu concerné, pourvu que soit nécessaire une telle communication des données sous une forme identifiable aux fins des statistiques et que l'organisme qui les reçoit s'engage par écrit à s'abstenir de toute communication ultérieure des renseignements sous une forme qui risque vraisemblablement de permettre l'identification des individus concernés.

---

[33] En Alberta et en Colombie-Britannique, une exception de taille a trait aux « renseignements personnels des employés » (« *employee personal information* » ou « *personal employee information* »). En Colombie-Britannique, la collecte, l'usage et la divulgation de ces renseignements pourrait se faire sans le consentement de l'individu concerné lorsqu'il s'agit d'une utilisation raisonnable aux fins d'établir, de gérer ou de mettre fin à une relation de travail entre l'organisation et l'individu : *Personal Information Protection Act*, S.B.C. 2003, c. 63, art. 13, 16 et 19 [Colombie-Britannique]. De plus, en Alberta, la collecte, l'usage et la divulgation de ces renseignements ne nécessitent pas le consentement de l'individu concerné si ce dernier est un employé et aux fins de recrutement. La collecte doit toutefois être raisonnable et ne consister qu'en de l'information liée uniquement à un emploi futur ou à une relation de travail bénévole. Dans le cas des employés actuels, un avis raisonnable doit être donné indiquant que l'information sera collectée, utilisée ou divulguée de même que les fins auxquelles ces opérations sont destinées : *Personal Information Protection Act*, S.A. 2003, c. P-6.5, art. 15, 18 et 21 [Alberta].

[34] *Infra*, p. 11 et 12.

[35] Parmi les cas où un responsable peut refuser la communication des renseignements personnels demandés, figurent les renseignements protégés par le secret professionnel et les dossiers médicaux.

Dans le cas particulier des organismes statistiques national et provinciaux, ils sont investis de pouvoirs exorbitants, tels celui de conclure des accords spéciaux relatifs à l'échange de renseignements recueillis entre organismes statistiques fédéral-provinciaux, ou entre organismes statistiques et tout ministère, municipalité ou autre personne morale. De plus, les individus recensés sont tenus, sous peine de sanction pénale, de retourner les réponses dûment certifiées exactes à l'organisme statistique national ou provincial quant aux renseignements que les lois lui autorisent à obtenir. Quant à la cueillette des statistiques criminelles, c'est le greffier des tribunaux pénaux, le directeur de chaque pénitencier et de chaque maison de correction ou le shérif de chaque comté, district ou autre circonscription qui remplit et transmet les questionnaires reçus au sujet des affaires pénales ou des prisonniers.

1.4 Autorités de contrôle

Au fédéral comme au niveau de chaque province et territoire, la protection des renseignements personnels est avant tout assujettie à la surveillance administrative d'une autorité indépendante qui relève directement du Parlement ou des législatures provinciales (i). Les cours de justice exercent un contrôle judiciaire à l'encontre des décisions rendues par cet organisme de surveillance ainsi qu'un rôle plus direct dans la garantie du respect de la vie privée au sens large (ii).

1.4.1 Les organismes de surveillance administrative

Qu'il soit appelé dans la plupart des cas le Commissariat à l'information et à la protection de la vie privée (« *Information and Privacy Commissioner* »), la Commission d'accès à l'information au Québec, le *Review officer* en Nouvelle-Écosse, ou l'ombudsman au Manitoba, il s'agit d'un organisme indépendant du gouvernement fédéral, provincial ou territorial et qui est chargé de l'application des deux (2) lois principales en matière de protection des renseignements personnels dans les secteurs public et privé.

Les commissaires sont nommés, pour un terme fixe renouvelable, par le gouvernement (fédéral ou provincial) après approbation par résolution du Parlement ou des législatures provinciales. La durée de leur mandat varie entre cinq (5) et sept (7) ans[36]. Les pouvoirs des commissaires sont essentiellement les suivants :

- Ils reçoivent les plaintes des justiciables alléguant le non-respect des lois par les organismes responsables dans le traitement de leurs renseignements personnels, ou encore prennent l'initiative d'une plainte s'ils ont des motifs raisonnables de croire qu'une enquête devrait être menée sur une question relative à l'application des lois;
- Ils mènent les enquêtes en donnant aux plaignants et aux responsables de l'organisme concerné la possibilité de présenter leurs observations, en exigeant la production des éléments de preuve (indépendamment de leur admissibilité devant les tribunaux), en assignant les témoins à comparaître devant eux et en examinant tout renseignement *a priori* protégé ;
- Dans les cas où ils concluent au bien-fondé d'une plainte, les Commissaires présentent aux organismes impliqués les conclusions de leurs enquêtes, leur adressent toute

[36] En Terre-Neuve-et-Labrador, le mandat du commissaire est seulement de deux (2) ans, renouvelable par ailleurs: *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1, art. 42.2(1).

recommandation jugée appropriée et assument à l'occasion le suivi quant à la mise en œuvre des recommandations. Les Commissaires peuvent aussi tenter de régler les plaintes à l'amiable, par le biais de la négociation et de discussions persuasives, telles que la médiation ou la conciliation. Dans les cas qui demeurent toujours non résolus, les Commissaires peuvent saisir de la question soit la Cour fédérale, soit les cours supérieures provinciales ou territoriales[37];

- Lorsqu'une plainte est jugée non fondée par les Commissaires, cette décision peut être portée, selon le cas, en révision judiciaire devant la Cour fédérale ou les cours supérieures provinciales ou territoriales.

D'un autre côté, les Commissaires ont également pour rôle de promouvoir le respect de la vie privée auprès du grand public en lui offrant des programmes d'information et d'encourager les organismes à élaborer des politiques internes détaillées sur la problématique.

1.4.2 Le rôle des autorités judiciaires dans la protection des renseignements personnels

Comme nous avons vu, les cours supérieures de justice n'interviennent qu'au second palier pour assurer l'application des lois sur la protection des renseignements personnels. Elles siègent soit sur la saisine des Commissaires (lorsque les plaintes ne peuvent se résoudre à ce niveau), soit en révision des décisions rendues par les organismes administratifs indépendants, conformément au pouvoir inhérent de surveillance et de contrôle de la légalité des décisions rendues par les tribunaux inférieurs et déclarées sans appel.

Quant au respect de la vie privée au sens large, dont la protection est garantie à des degrés variables par les droits communs privés provinciaux, les recours en responsabilité civile fondée sur la faute ainsi que les actions en délit civil des provinces de common law, sont portés devant les tribunaux de droit commun.

2. Protection de la personne lors de traitements de données personnelles à des fins administratives ou judiciaires

Par ailleurs, le Canada s'est doté d'un régime spécial pour la protection de données personnelles relatives aux infractions criminelles et intéressant la Sûreté de l'État (a) ainsi que pour le traitement des données biométriques (b).

---

[37] Au Manitoba, la plainte préalablement traitée par l'ombudsman est déférée plutôt à un arbitre en matière d'accès à l'information et de protection de la vie privée, dont la décision pourra être portée ensuite en révision judiciaire : *Loi sur l'accès à l'information et la protection de la vie privée*, C.P.L.M. c. F175, art. 58.1 et suiv. [Manitoba]. Au Québec, les lois prévoient un mécanisme de révision interne. La Commission d'accès à l'information comporte deux (2) sections, la section de surveillance et la section juridictionnelle. C'est la section juridictionnelle qui décide en premier lieu des demandes de révision des décisions rendues par la section de surveillance. La décision rendue par la section juridictionnelle doit être homologuée par la Cour supérieure pour être exécutoire; cette décision est sans appel sur une question de fait, tandis qu'elle pourra être portée en appel devant un juge de la Cour du Québec sur une question de droit ou de compétence. Dans tous les cas, une révision judiciaire devant la Cour supérieure est toujours possible : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, art. 103 et suiv.; *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, art. 41.1 et suiv. [Québec]

2.1 Protection lors de traitement de données intéressant la sûreté de l'État ou de données relatives aux infractions criminelles

Les renseignements personnels intéressant la sûreté de l'État (i) ainsi que les données relatives aux infractions criminelles (ii) font l'objet de conditions plus strictes.

2.1.1 Divulgation de renseignements intéressant la sûreté de l'État

De prime abord, toute institution fédérale peut refuser la communication des renseignements personnels dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales, à la défense du Canada ou d'États alliés ou associés voire à la prévention et à la répression des crimes[38]. Par ailleurs, certaines données sont classées inconsultables par décret, tels les dossiers du renseignement et de la sécurité[39], les dossiers opérationnels de renseignements sur la criminalité[40], les dossiers d'enquête du Service canadien du renseignement de sécurité[41] ainsi que les dossiers des enquêtes relatives à la sécurité nationale[42]. Les entreprises fédérales du secteur privé sont par contre tenues de communiquer à une institution gouvernementale tout renseignement que celle-ci soupçonne être afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales ou lorsqu'il y a des motifs raisonnables de soupçonner que le renseignement est lié à la perpétration d'une infraction de recyclage des produits de la criminalité ou de financement des activités terroristes[43]. Le cas échéant, l'institution gouvernementale peut refuser d'acquiescer à la demande d'accès de l'individu concerné relatif aux renseignements le concernant[44]. À l'échelle provinciale et territoriale, les organismes publics peuvent[45] refuser de donner communication d'un renseignement ayant des incidences sur l'administration de la justice et la sécurité publique ou de l'État. À l'égard de l'individu intéressé, le droit d'accès est restreint aux extraits de renseignements ne faisant pas l'objet de l'interdiction.

2.1.2 Gestion des dossiers criminels

Au Canada, le principe de la publicité du procès et des accusations, consacré à l'article 11*d*) de la Charte canadienne, emporte le droit pour quiconque du grand public d'avoir accès au plumitif et dossiers de cour. À ce jour, seule la province du Québec prévoit un tempérament à ce principe : conformément la *Directive concernant la gestion de certains renseignements contenus dans les registres et relevés informatisés en matière criminelle* (« la Directive D-21 »),

---

38 *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21, art. 21 et 22(1) [fédéral].

39 *Décret no 5 sur les fichiers de renseignements personnels inconsultables (DN)*, DORS/85-38.

40 *Décret no 13 sur les fichiers de renseignements personnels inconsultables (GRC)*, DORS/90-149.

41 *Décret no 14 sur les fichiers de renseignements personnels inconsultables (SCRS)*, DORS/92-688.

42 *Décret no 25 sur les fichiers de renseignements personnels inconsultables (GRC)*, DORS/93-272.

43 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, art. 7(3)c.1), c.2) et d).

44 *Id.*, art. 9.

45 À l'exception de la province du Québec, où le refus est obligatoire : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, art. 28 – 29.1.

une personne qui a été l'objet d'une accusation criminelle peut, en certaines circonstances[46], demander que soient rendus inaccessibles au public des renseignements contenus dans les registres et relevés informatiques tenus par le ministère de la Justice[47].

Selon le droit canadien, toute personne déclarée coupable d'avoir commis une ou plusieurs infractions criminelles en contravention des lois ou règlements fédéraux (comme le *Code criminel* ou la *Loi réglementant certaines drogues et autres substances*[48]) possède un casier judiciaire. Il s'agit d'une inscription dans un registre administré par la Gendarmerie Royale du Canada (GRC), contenant le sommaire des verdicts de culpabilité d'un individu. Les lois fédérales, provinciales ou territoriales ne protègent qu'imparfaitement la discrimination fondée sur l'existence d'un casier judiciaire, qui n'est pas un motif de distinction illicite reconnu d'un océan à l'autre[49]. Il est cependant possible, à certaines conditions et à l'expiration d'une période plus ou moins longue dépendamment du type de condamnations, de requérir une suspension de son casier judiciaire auprès de la Commission nationale des libérations conditionnelles[50]. Une fois le casier suspendu, le fichier du requérant est classé à part des autres dossiers ou relevés relatifs à des affaires pénales, et il devient en principe interdit de le communiquer, sous réserve des impératifs liés à l'administration de la justice, à la sûreté ou la sécurité du Canada ou d'un État allié ou associé au Canada[51]. Dans le même ordre d'idées, la Commission retire du fichier automatisé des relevés de condamnations criminelles géré par la GRC toute mention

---

[46] Ces circonstances sont les suivantes : a) l'acquittement pour une raison autre qu'un verdict de non-responsabilité criminelle pour cause de troubles mentaux, à l'expiration de deux mois suivant l'expiration du délai d'appel ou à l'expiration de trois mois suivant l'issue de toutes les procédures d'appel; b) l'accusation est rejetée autrement que par l'acquittement ou est retirée, à l'expiration d'un an suivant la date du rejet ou de retrait; c) l'accusation est suspendue sans qu'aucune procédure ne soit prise contre l'accusé, à l'expiration d'un an suivant la date de l'arrêt des procédures; d) la libération de l'accusé à l'enquête préliminaire ou sur défense d'autrefois acquis ou d'autrefois convict, à l'expiration d'un an suivant la date de la libération; e) l'absolution inconditionnelle, à l'expiration d'un an suivant la date de l'ordonnance; f) l'absolution sous conditions, à l'expiration de trois ans suivant la date de l'ordonnance sous conditions; g) la libération inconditionnelle à la suite d'un verdict de non-responsabilité criminelle pour cause de troubles mentaux, à l'expiration d'un an suivant la date de la décision; h) la libération sous réserve des modalités que le tribunal ou la Commission d'examen juge indiquées à la suite d'un verdict de non-responsabilité criminelle pour cause de troubles mentaux, à l'expiration de trois ans suivant la date de la décision; i) l'engagement de ne pas troubler l'ordre public en vertu de l'article 810 du Code criminel, à l'expiration d'un an suivant l'écoulement de la période mentionnée à l'engagement.

[47] Voir aussi les termes de la transaction entérinée dans l'affaire *Ostiguy*, recours collectif exercé contre le *Procureur général du Québec*, le Procureur général du Canada ainsi que les Villes de Montréal, de Laval et de Longueuil (2008), en ligne : <http://www.justice.gouv.qc.ca/francais/ministere/avis/2008/transaction.pdf>.

[48] *Loi réglementant certaines drogues et autres substances*, L.C. 1996, c. 19.

[49] En fait, seule l'Ontario ainsi que le Yukon, le Nunavut et les Territoires du Nord-Ouest prévoient une protection législative contre la discrimination fondée sur « l'existence d'un casier judiciaire » (Ontario : *Code des droits de la personne*, L.R.O. 1990, c. H.19), « l'existence d'accusations au criminel ou d'antécédents criminels » (Yukon : *Loi sur les droits de la personne*, L.R.Y. 2002, c. 116, art. 7*i*)), « l'état de personne condamnée puis réhabilitée » (Nunavut : *Loi sur les droits de la personne*, L.Nun. 2003, c. 12, art. 7(1) *in fine*) ou « la condamnation qui peut faire l'objet d'un pardon ou d'une suspension du casier » (Territoires du Nord-Ouest : *Loi sur les droits de la personne*, L.T.N.-O. 2002, c. 18, art. 5(1) *in fine*). Au Québec, une déclaration de culpabilité est assujettie à un régime de protection à part, de portée plus restreinte : voir *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 18.2.

[50] *Loi sur le casier judiciaire*, L.R.C. 1985, c. C-47, en particulier les articles 3 - 4.4.

[51] *Id.*, art. 6 et 8; dans certaines circonstances, la Commission nationale des libérations conditionnelles peut par la suite révoquer la suspension du casier (voir art. 7), ou encore certains faits peuvent entraîner ultérieurement la nullité de cette suspension (voir art. 7.2).

d'un dossier ou relevé attestant d'une absolution à l'écoulement d'un (1) an suivant la date de l'ordonnance inconditionnelle ou de trois (3) ans suivant la date de l'ordonnance sous conditions[52]. Au reste, les antécédents criminels sont par ailleurs assujettis au régime général prévu dans les deux (2) lois principales sur la protection des renseignements personnels des secteurs public et privé.

En Saskatchewan, la *Public Disclosure Act*[53] prévoit en outre la constitution d'un comité chargé d'examiner, sur demande des services de police locaux et après avoir donné aux personnes intéressées l'occasion de se faire entendre, l'opportunité de communiquer certains renseignements identifiant de grands criminels pour protéger le public et les victimes.

3.1 Protection de données biométriques

Les mesures ou caractéristiques biométriques sont des renseignements personnels, dès lors qu'elles concernent un individu et permettent de l'identifier. Relativement au traitement des renseignements biométriques, diverses lois fédérales encadrent le prélèvement de données biométriques chez des accusés (i) et dans le cadre du programme d'immigration et de protection des réfugiés au Canada (ii). Des mesures législatives provinciales sont également pertinentes quant à la gestion des données biométriques par des entreprises privées (iii).

3.1.1 Prélèvement de données biométriques chez les accusés

Dans le contexte criminel et pénal, la ***Charte canadienne des droits et libertés*** élève au rang constitutionnel le droit de chacun « à la protection contre les fouilles, les perquisitions ou les saisies abusives » (art. 8). L'étendue de ce droit est circonscrite par le concept d'expectative raisonnable, appréciée sous un angle subjectif, qui est par ailleurs éminemment dépendante de l'ensemble des circonstances objectives dans ce contexte particulier[54]. La violation de ce droit par les autorités policières pourrait entraîner l'exclusion des éléments de preuve ainsi recueillis aux termes de l'article 24(2) de la Charte canadienne si, eu égard à toutes les circonstances, leur utilisation était susceptible de déconsidérer l'administration de la justice[55]. En principe, lorsqu'elle peut être obtenue, une autorisation préalable – qu'elle soit judiciaire ou législative – est une condition préalable à la validité d'une fouille, d'une perquisition et d'une saisie[56].

Depuis 1995, une autorisation judiciaire peut être obtenue en vertu des articles 487.04 et suivants du ***Code criminel*** aux fins d'ordonner le prélèvement d'échantillons biologiques pour analyse génétique, lorsqu'il existe des motifs raisonnables de croire que certaines infractions

---

52 *Id.*, art. 6.1.

53 *Public Disclosure Act*, S.S. 1996, c. P-36.1.

54 *R.* c. *Cole*, 2012 CSC 53. La portée de cette protection constitutionnelle n'est pas limitée à la seule preuve corporelle, mais touche également aux éléments de preuve matériels, telle la saisie d'un ordinateur dans l'affaire *Cole*.

55 Les critères d'appréciation ont été définis dans l'arrêt *R.* c. *Grant*, [2009] 2 R.C.S. 353.

56 Principe établi dans l'arrêt *Hunter et autres* c. *Southam Inc.*, [1984] 2 R.C.S. 145, à moins d'une fouille consécutive à une arrestation (*R.* c. *Stillman*, [1997] 1 R.C.S. 607) ou à une détention (*R.* c. *Mann*, [2004] 3 R.C.S. 59).

désignées[57] avaient été commises et qu'une analyse génétique de la substance corporelle apportera des preuves utiles en ce qui concerne la perpétration de l'infraction. En matière militaire, un juge militaire peut pareillement ordonner, par délivrance d'un mandat, le prélèvement d'échantillons biologiques à des fins médicolégales dans certaines conditions[58].

La ***Loi sur l'identification des criminels***[59] oblige de son côté toute personne inculpée – avant même qu'elle ne soit reconnue coupable – à se soumettre à un processus de prise d'empreintes digitales et de photos, pour lequel le recours à la force est expressément permis. Le refus d'y obtempérer, sans excuse légitime, constitue une infraction criminelle et rend la personne passible d'un emprisonnement maximal de deux (2) ans[60]. Cette procédure a été jugée conforme à la Charte canadienne[61]. Les empreintes digitales d'un individu sont recueillies par le corps policier responsable de l'enquête et transmis au Service d'identité judiciaire de la GRC. À la réception des empreintes digitales, le Service d'identité judiciaire de la GRC attribue un numéro de dossier FPS (*Finger Print Section*), et l'individu devient fiché à l'intérieur du Centre d'information de la police canadienne (CIPC). Les rudiments d'un éventuel casier judiciaire sont là. Ce bertillonnage est détruit d'office lorsque la personne qui y est soumise est inculpée d'une infraction qualifiée de contravention au sens de la *Loi sur les contraventions*[62]. Dans les autres cas, malgré l'arrêt des procédures, un acquittement, la non-judiciarisation, voire le retrait des accusations, la « fiche signalétique » n'est pas automatiquement détruite par les corps policiers. Ces derniers procèdent différemment en vertu des politiques administratives internes[63]. En général, le justiciable doit faire une demande de destruction par écrit au corps policier responsable de l'enquête qui a procédé à la prise des empreintes digitales. Le corps de police achemine alors cette demande à la GRC pour la destruction des empreintes comme le retrait des informations du CIPC.

---

57 Il s'agit des infractions primaires et secondaires listées à l'article 487.04 du *Code criminel*, notamment des infractions graves contre la personne ou d'ordre sexuel.

58 Voir la *Loi sur la défense nationale*, L.R.C. 1985, c. N-5, art. 196.11 et suiv.

59 *Loi sur l'identification des criminels*, L.R.C. 1985, c. I-1, en particulier l'article 2.

60 *Code criminel*, L.R.C. 1985, c. C-46, art. 145(4).

61 *R.* c. *Beare*; *R.* c. *Higgins*, [1988] 2 R.C.S. 387, par. 40 et 41 : « […] pour beaucoup de gens, il est humiliant d'être soumis à un prélèvement d'empreintes digitales, et il est indéniable que pour beaucoup le procédé est déplaisant. Mais il faut rappeler que l'obligation, d'intérêt public, de faire respecter la loi contraint l'individu à se soumettre à d'autres procédures tout aussi déplaisantes. Il est déplaisant d'être accusé d'une infraction, et cela est même extrêmement désagréable dans le cas de certains crimes, sans parler de la honte de l'arrestation, de la détention et de l'obligation de répondre de l'inculpation au procès. […] Les flétrissures liées à ces aspects ordinaires de l'application de la loi et de la justice criminelle dépassent de loin tout sentiment d'indignité que susciterait la prise d'empreintes digitales. Et pourtant je ne pense pas que, lorsqu'il y a des motifs probables et raisonnables de croire qu'une personne a commis une infraction, on puisse sérieusement soutenir que la soumettre à l'une ou l'autre de ces procédures viole les principes de justice fondamentale. »

62 *Loi sur l'identification des criminels*, L.R.C. 1985, c. I-1, art. 4 ; voir la liste des « contraventions » au sens de la *Loi sur les contraventions* (L.C. 1992, c. 47) à l'annexe I du *Règlement sur les contraventions*, DORS/96-313.

63 Selon la Cour d'appel de l'Ontario, les corps policiers ne sont pas tenus de procéder à la destruction des fiches signalétiques de leur propre initiative : *R.* c. *Doré*, [2002] OJ n° 2845 (Ont. C.A.). En cas d'antécédents judiciaires, de troubles mentaux ou de certains crimes graves (meurtre, agression sexuelle, pornographie juvénile, gangstérisme…), la police peut refuser une demande de destruction.

La ***Loi sur l'identification par les empreintes génétiques***[64] a reçu la sanction royale le 10 décembre 1998. Son objet, faciliter la découverte, l'arrestation et la condamnation rapides des contrevenants au nom de la protection de la société et de l'administration de la justice. Est établie une banque nationale de données génétiques – composée d'un fichier de criminalistique et d'un fichier des condamnés – tenue par le commissaire de la GRC. Le fichier de criminalistique contient les profils d'identification génétique établis à partir de substances corporelles trouvées sur les lieux du crime, tandis que le fichier des condamnés contient les profils d'identification génétique établis à partir des substances corporelles prélevées en vertu d'une ordonnance ou autorisation judiciaire[65].

Il est interdit de communiquer toute information contenue dans la banque de données, sauf pour les besoins de toute enquête relative à une infraction criminelle, et uniquement à un laboratoire ou organisme canadien chargé du contrôle d'application de la loi. Pour sa part, le commissaire de la GRC compare le profil d'identification génétique déposé aux deux fichiers avec les profils qui sont déjà dans la banque de données. Il peut également le faire sur réception d'un profil d'identification génétique émanant du gouvernement d'un État étranger, d'une organisation internationale de gouvernements, ou d'un de leurs organismes, de même que de communiquer les profils canadiens aux gouvernements étrangers ou organisations internationales, dans certaines circonstances. Toute utilisation des résultats de l'analyse génétique contenus dans le fichier des condamnés autre qu'en conformité avec la loi est par ailleurs prohibée[66]. L'accès à l'information contenue dans la banque de données est pareillement limité au personnel d'un laboratoire et toute personne que le commissaire de la GRC estime indiquée[67]. Le fichier de criminalistique est rendu inaccessible une fois pour toutes lorsque la victime d'une infraction désignée a fait l'objet de l'enquête ou que la personne n'est plus considérée comme un suspect[68]. En principe, tout renseignement contenu dans le fichier des condamnés y est conservé pour une période indéterminée[69].

Pour sa part, la ***Loi sur l'enregistrement de renseignements sur les délinquants sexuels***[70], entrée en vigueur le 15 décembre 2004, exige l'enregistrement de certains renseignements sur les délinquants sexuels afin d'aider les services de police à prévenir les crimes de nature sexuelle et à enquêter sur ceux-ci. Aux termes de cette loi, une personne déclarée coupable d'une infraction désignée de nature sexuelle[71] et qui fait l'objet d'une ordonnance rendue en application de l'article 490.012 du *Code criminel* ou de l'article 227.01 de la *Loi sur la défense nationale*, est tenue de comparaître au bureau d'inscription desservant le secteur de la province

---

64 *Loi sur l'identification par les empreintes génétiques*, L.C. 1998, c. 37.

65 *Id.*, art. 5.

66 *Id.*, art. 6.

67 *Id.*, art. 7.

68 *Id.*, art. 8.1.

69 *Id.*, art. 9.

70 *Loi sur l'enregistrement de renseignements sur les délinquants sexuels*, L.C. 2004, c. 10.

71 Seules les infractions désignées aux alinéas *a*), *c*), *c.1*), *d*) ou *e*) de la définition d'infraction désignée de l'article 490.011(1) du *Code criminel* font l'objet d'une ordonnance d'enregistrement automatique. Les autres infractions désignées nécessitent toujours une demande du poursuivant.

où se trouve sa résidence principale, puis de fournir les renseignements de base suivants qui seront versés au registre national géré par la GRC[72] :

- ses nom et prénom et tout nom d'emprunt qu'il utilise;
- sa date de naissance et son sexe;
- l'adresse et le numéro de téléphone de sa résidence principale et de toute résidence secondaire;
- l'adresse et le numéro de téléphone de tout lieu où ses services ont été retenus à titre de salarié, d'agent contractuel ou de bénévole ainsi que le nom de son employeur et le type de travail effectué;
- le cas échéant, le fait qu'il est officier ou militaire du rang des Forces canadiennes, et l'adresse et le numéro de téléphone de son unité;
- l'adresse de tout établissement d'enseignement où il est inscrit;
- le numéro de tous ses téléphones mobiles ou téléavertisseurs;
- sa taille, son poids et la description de ses marques physiques distinctives;
- le numéro de la plaque d'immatriculation, la marque, le modèle, le type de carrosserie, l'année de fabrication et la couleur de tout véhicule à moteur immatriculé à son nom ou qu'il utilise régulièrement.

De plus, toutes les personnes condamnées à l'étranger pour des infractions à caractère sexuel doivent également s'inscrire au registre national en arrivant au Canada, de sorte que les autorités policières canadiennes pourront avertir les autres services policiers étrangers des déplacements d'un délinquant sexuel considéré à risque élevé dans leur ressort[73].

Les renseignements qui y sont inscrits seront conservés pour une période indéterminée, à moins d'un acquittement final de l'intéressé ou pardon absolu accordé en vertu de la prérogative royale de clémence ou d'autres cas limitativement prévus à l'article 15 de la loi.

En revanche, dans l'intérêt du respect de la vie privée des délinquants sexuels ainsi que de leur réhabilitation et de leur réinsertion sociale, le public n'a pas accès au registre des délinquants sexuels. Toute consultation, comparaison, communication, liaison et fusion des renseignements recueillis dans le registre national est interdite, sauf à une personne visée à l'article 16 de la loi, tel un service de police chargé d'enquêter sur la perpétration d'un crime sexuel ou un agent autorisé de la GRC dans le cadre de la gestion du registre national. Pour des travaux de recherche et de statistique, le commissaire de la GRC peut autoriser, à certaines conditions, la consultation de renseignements enregistrés, la comparaison de ces renseignements avec d'autres, la liaison par voie électronique de ces renseignements avec d'autres contenus dans un ordinateur ou leur fusion avec de tels renseignements[74].

L'Ontario est présentement la seule province canadienne à établir son propre registre de délinquants sexuels par la ***Loi Christopher de 2000 sur le registre des délinquants sexuels***

---

72 *Loi sur l'enregistrement de renseignements sur les délinquants sexuels*, L.C. 2004, c. 10, art. 5(1).

73 Voir *Id.*, art. 3(1) quant à la définition d'un « délinquant sexuel ».

74 *Id.*, art. 13.

(ci-après la « Loi Christopher »)[75], proclamée le 23 avril 2001. Le registre ontarien est géré par la Police provinciale de l'Ontario et a été conçu afin de fournir aux corps policiers les renseignements et les outils d'enquête nécessaires pour prévenir et élucider les crimes de nature sexuelle. Il s'agit d'un régime dérogatoire[76] à celui prévu à la *Loi sur l'accès à l'information et la protection de la vie privée*[77] et la *Loi sur l'accès à l'information municipale et la protection de la vie privée*[78]. L'inscription est automatique pour les délinquants qui résident en Ontario et sont déclarés coupables d'une infraction sexuelle, aux résidents ontariens qui ont reçu un verdict de non-responsabilité criminelle pour cause de troubles mentaux ainsi qu'aux jeunes contrevenants condamnés à une peine applicable aux adultes pour une des infractions sexuelles désignées. Une personne visée par la loi fédérale sur l'enregistrement des délinquants sexuels, où qu'elle se trouve au Canada, doit aussi se conformer à la loi ontarienne[79]. Les renseignements qui doivent être inscrits au registre sont énumérés à l'article 2(1) du *Règlement de l'Ontario 69/01*. Un délinquant sexuel a le droit de consulter les renseignements le concernant ainsi que le droit de les faire corriger, au besoin[80]. En Ontario, les policiers sont autorisés à consulter les renseignements contenus dans le registre provincial pour prévenir les crimes à caractère sexuel ou encore pour vérifier l'exactitude des informations qui s'y trouvent. Le public n'a pas accès à la banque de données du registre, et toute divulgation non autorisée de son contenu constitue une infraction[81].

3.2.2 Dans le cadre du programme canadien d'immigration et de protection des réfugiés

En raison de l'augmentation du volume de demandes, de l'évolution des tendances en matière de déplacement, de la multiplication du nombre de fraudes d'identité ainsi que des moyens de plus en plus perfectionnés d'y parvenir, le recours à la biométrie renforcerait le programme d'immigration du Canada et aiderait à protéger la sécurité des Canadiens, en offrant aux agents des visas davantage de certitude lors du filtrage des demandeurs et en leur permettant de confirmer plus aisément l'identité des personnes. Dans cette visée, la *Loi visant à protéger le système d'immigration du Canada*[82], qui a reçu la sanction royale le 28 juin 2012, habilite le gouvernement à demander aux ressortissants de certains pays ou de territoires de fournir des données biométriques. La collecte de ces renseignements suivra la procédure qui aura été établie par règlement. En outre, celui-ci décrira en particulier à qui s'appliqueraient les exigences en matière de biométrie, les frais de prélèvement biométrique ainsi que les utilisations et les divulgations prévues de ces données biométriques à des fins d'application de la *Loi sur l'immigration et la protection des réfugiés*[83].

---

75 *Loi Christopher de 2000 sur le registre des délinquants sexuels*, L.O. 2000, c. 1.

76 *Id.*, art. 13.

77 *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, c. F.31 [Ontario].

78 *Loi sur l'accès à l'information municipal et la protection de la vie privée*, L.R.O. 1990, c. M.56 [Ontario].

79 *Loi Christopher de 2000 sur le registre des délinquants sexuels*, L.O. 2000, c. 1, art. 8.

80 *Id.*, art. 6(1) et (3).

81 *Id.*, art. 10.

82 *Loi visant à protéger le système d'immigration du Canada*, L.C. 2012, c. 17.

83 *Loi sur l'immigration et la protection des réfugiés*, L.C. 2001, c. 27.

Conformément aux modifications proposées[84] à l'actuel *Règlement sur l'immigration et la protection des réfugiés*[85], seuls les demandeurs d'un visa de résidence temporaire ou d'un permis d'études ou de travail qui sont citoyens d'un pays ou titulaires d'un titre de voyage d'un territoire figurant sur une liste préétablie[86]. Ces demandeurs devront se présenter en personne à un point de collecte de renseignements afin de soumettre leurs empreintes digitales et de se faire photographier. Les dispositions réglementaires proposées autoriseraient la comparaison des empreintes digitales prélevées aux fins d'immigration aux empreintes latentes (non identifiées, telles celles recueillies sur la scène d'un crime), aux empreintes des criminels ou à d'autres empreintes présentant un intérêt pour les enquêtes policières. En cas de correspondance des empreintes, la GRC pourra utiliser ou communiquer à un autre organisme canadien chargé du contrôle de l'application de la loi les empreintes prélevées aux fins d'immigration et les renseignements personnels connexes.

Au reste, ces nouvelles exigences seront introduites progressivement sur plusieurs mois, du 2 septembre 2013 au 7 décembre 2013.

3.3.3 Autres mesures provinciales relativement au traitement des données biométriques

Finalement, précisons qu'au Québec, nul ne peut exiger la vérification ou la confirmation de l'identité d'une personne au moyen de la biométrie, sans le consentement exprès de la personne concernée[87]. Dans tous les cas, la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. Celle-ci peut rendre toute ordonnance pour déterminer la confection, l'utilisation, la consultation, la communication et la conservation, y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée[88].

Bilan et perspective

À la lumière de ce qui précède, nous pouvons conclure que, malgré l'apparente diversité des législations fédérales, provinciales ou territoriales quant au traitement des données personnelles – une diversité inhérente au caractère fédéral de l'État canadien, les régimes généraux relatifs à la protection des renseignements personnels convergent en fin de compte

---

84 Pour un résumé de l'étude d'impact de la réglementation, voir *Règlement modifiant le Règlement sur l'immigration et la protection des réfugiés*, (2012) 146 Gaz. Can. I, en ligne : <http://www.gazette.gc.ca/rp-pr/p1/2012/2012-12-08/html/reg2-fra.html>.

85 *Règlement sur l'immigration et la protection des réfugiés*, DORS/2002-227.

86 Il s'agirait du territoire de l'Autorité palestinienne et des pays suivants : l'Afghanistan, l'Albanie, l'Algérie, l'Arabie saoudite, le Bangladesh, la Birmanie, le Cambodge, la Colombie, la République démocratique du Congo, l'Égypte, l'Érythrée, le Haïti, l'Irak, l'Iran, la Jamaïque, la Jordanie, le Laos, le Liban, la Libye, le Nigéria, le Pakistan, la Somalie, le Soudan, le Soudan du Sud, le Sri Lanka, la Syrie, la Tunisie, le Viêt Nam et le Yémen.

87 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C.1.1, art. 44.

88 *Id.*, art. 45.

vers nombre de points communs : dans tous les cas, la protection est axée sur les opérations ponctuelles (la collecte, la divulgation, l'usage et la destruction) effectuées sur les données personnelles et consacre le droit des individus concernés à y exercer un certain contrôle (droit d'être informé, nécessité d'y consentir, droits d'accès et de rectification).

Avec l'avènement de l'ordinateur et de l'Internet, le droit au respect de la vie privée ainsi que le traitement des données biométriques (au criminel et en matière d'immigration) poseront vraisemblablement de nouveaux défis aux gestionnaires de tous les niveaux. Bien que l'on ne soit peut-être pas encore à invoquer un régime spécifique à l' « habeas corpus numérique », le régime de protection traditionnel est certainement appelé à se perfectionner au rythme de nouvelles possibilités qu'offrent les technologies et l'espace numérique…