



LA FOUILLE D'APPAREILS ÉLECTRONIQUES AU TRAVAIL

SYNTHÈSE PARTIELLE DE LA JURISPRUDENCE SUR LE DROIT FONDAMENTAL DE LA PERSONNE À LA VIE PRIVÉE CONCERNANT LA FOUILLE EN CONTEXTE D'EMPLOI

Marie-Josée Legault, professeure titulaire de relations industrielles, TÉLUQ

RÉSUMÉ	3
QU'EST-CE QUE LE DROIT À LA VIE PRIVÉE EN CONTEXTE D'EMPLOI?	3
Qu'est-ce que le droit à la vie privée?	3
Le contexte d'emploi et la relation de subordination	4
Les limites qu'imposent les droits fondamentaux	5
Le statut particulier des droits fondamentaux	6
Les lois sur la protection des renseignements personnels des employés	7
<i>La Loi sur la protection des renseignements personnels dans le secteur privé</i>	<i>8</i>
<i>Les lois fédérales.....</i>	<i>9</i>
LE PROBLÈME VISÉ.....	10
Le contenu des appareils électroniques, la vie privée et les intérêts de l'employeur	10
Le droit à la vie privée inclut-il la protection des renseignements personnels emmagasinés dans un ordinateur <i>personnel</i> ?	11
Une obligation qui restreint le droit à la vie privée de l'employé : le devoir de loyauté	14
Quel est le pouvoir de fouille de l'employeur qui soupçonne une rupture de l'obligation de loyauté? ..	14
QUEL EST LE RECOURS DE L'EMPLOYEUR LÉSÉ?	15
L'ordonnance d'injonction	16
La question de l'urgence dans les cas de concurrence déloyale	16
Le recours en dommages-intérêts	19
LE RECOURS DE L'EMPLOYÉ LÉSÉ	20
Contester l'admissibilité d'une preuve.....	20
Contester l'atteinte à la vie privée	20

LE DROIT DE FOUILLE EN CONTEXTE D'EMPLOI.....	20
Le droit de fouille de l'employeur et le droit à la vie privée.....	20
Le droit de fouille des appareils informatiques.....	22
Qui peut fouiller un appareil informatique?	23
QUAND L'EMPLOYEUR EST-IL EN DROIT DE FOUILLER UN APPAREIL INFORMATIQUE?	23
La fouille autorisée ou le consentement.....	25
<i>Le consentement explicite</i>	25
<i>Le consentement implicite</i>	26
<i>En l'absence d'un consentement généralisé de la part des travailleurs</i>	27
L'employé pouvait-il entretenir une attente de vie privée à l'égard de l'information vérifiée par l'employeur?.....	28
<i>La propriété de l'ordinateur</i>	28
<i>La nature de l'information recherchée</i>	29
<i>L'endroit où l'information est emmagasinée</i>	29
<i>Les mesures technologiques de protection</i>	30
<i>Le fait que l'information a été effacée ou non</i>	30
L'EMPLOYEUR A-T-IL LE DROIT LÉGITIME DE FOUILLER?.....	31
Le motif justifiant la vérification.....	31
La nature de l'utilisation de l'ordinateur par l'employé.....	32
Le niveau d'autorité de la personne qui demande la vérification.....	33
Les moyens et procédés utilisés pour accéder à l'information.....	33
L'urgence d'agir pour l'employeur.....	34
QUEL EST LE RAISONNEMENT DU TRIBUNAL EN CAS DE PLAINTÉ?.....	35
La démarche axée sur la proportionnalité.....	35
Trois exemples d'application de la démarche axée sur la proportionnalité.....	36
<i>L'arrêt Cole : l'importance de l'information à caractère intime et personnel</i>	36
<i>La décision Pneus Touchette : justifier l'atteinte au droit à la vie privée</i>	38
<i>Images Turbo : le droit à la vie privée est limité pendant la relation d'emploi, mais pas après</i>	39
L'EMPLOYÉ PEUT-IL REFUSER LA FOUILLE?.....	40
LES CONDITIONS DE VALIDITÉ D'UNE POLITIQUE DE FOUILLE.....	41
Mettre en place une politique : un atout et une assurance.....	41
Réserver les appareils à l'usage professionnel.....	41
Les conséquences de l'autorisation de l'usage personnel.....	42
Prévoir la possibilité de fouille.....	43
La politique doit être connue de tous.....	43
L'application sans discrimination.....	43
Préciser qui peut fouiller.....	44
RÉFÉRENCES.....	44

RÉSUMÉ

Pour obtenir un résumé du contenu de cette synthèse, lisez tout simplement la table des matières, elle est conçue de façon à en résumer le contenu.

Quand vous aurez lu cette synthèse en entier, faites un test : relisez la table des matières, prenez quelques notes énonçant ce que vous retenir au sujet de chaque intertitre, puis vérifiez ce que vous avez écrit en relisant la synthèse. En effet, aux fins d'étude, une seule lecture ne suffit pas... Vous verrez alors ce qui vous a échappé. Tentez une deuxième fois de résumer le contenu de chaque intertitre.

QU'EST-CE QUE LE DROIT À LA VIE PRIVÉE EN CONTEXTE D'EMPLOI?

Qu'est-ce que le droit à la vie privée?

Le droit à la vie privée est considéré comme le droit pour un individu de contrôler ses renseignements personnels (Gratton, 2013, p. 6 et s.). La notion n'est pas formellement définie, mais on peut retenir ceci :

... le droit à l'anonymat et à l'intimité, ainsi que le droit à l'autonomie dans l'aménagement de sa vie personnelle et familiale ou encore le droit au secret et à la confidentialité. Font aussi partie du droit à la vie privée l'inviolabilité du domicile, l'utilisation de son nom, les renseignements liés à l'état de santé, la vie familiale et amoureuse et l'orientation sexuelle... (Hébert, 2013, p. 4).

La Cour suprême définit ainsi les composantes de la vie privée : le droit à l'anonymat, à l'intimité, à l'autonomie dans l'aménagement de sa vie personnelle et familiale ou encore le droit au secret et à la confidentialité (décision *Godbout c. Ville de Longueuil* [1997] (CSC), parag. 98).

Les citoyens du Québec sont protégés de l'atteinte à la vie privée par les articles 3, 35 et 36 du Code civil du Québec (CcQ), qui en font une faute civile, et par les articles 5, 9.1 et 24.1 de la Charte des droits et libertés de la personne du Québec, que nous verrons plus bas.

3. Toute personne est titulaire de droits de la personnalité, tel le droit à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation et de sa vie privée. (CcQ)

35. Toute personne a droit au respect de sa réputation et de sa vie privée.

Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise. (CcQ)

36. Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :

1. Pénétrer chez elle ou y prendre quoi que ce soit;
2. Intercepter ou utiliser volontairement une communication privée;

3. Capturer ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
4. Surveiller sa vie privée par quelque moyen que ce soit;
5. Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;
6. Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels. (CcQ)
37. Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation. (CcQ)



Dans le texte qui suit, nous désignons le Code civil du Québec par le sigle « CcQ ».



Vous pouvez consulter les lois canadiennes et québécoises gratuitement dans Internet. Chaque fois qu'une loi est citée, cherchez-la avec votre fureteur de recherche informatique; conservez un signet, enregistrez-en une copie dans votre ordinateur ou copiez le lien dans un document conçu à cette fin. C'est la meilleure façon d'avoir une version à jour, car les lois sont régulièrement modifiées. Assurez-vous d'obtenir la version intégrale et officielle. Il s'agit toujours d'une liste d'articles numérotés et non d'un texte ou d'articles de loi assortis de commentaires. Par exemple les lois du Québec portent la mention « © Éditeur officiel du Québec », ainsi que les suivantes : « Ce document a valeur officielle » et « À jour au... ». Les lois du Canada portent la mention « Dernière modification le... » et « Publié par le ministre... ».

Un justiciable au Québec peut donc obtenir des dommages-intérêts, et peut-être des dommages exemplaires, pour atteinte à la vie privée.

Le contexte d'emploi et la relation de subordination

L'article 2085 CcQ définit le **contrat de travail** et permet de connaître ses trois éléments constitutifs : 1) l'existence d'une prestation de travail; 2) une rémunération en contrepartie de cette prestation, quelle qu'en soit la forme, ce qui exclut seulement le travail bénévole; 3) la présence d'un lien de **subordination juridique** entre l'employeur et l'employé quant à l'exécution du contrat (Gagnon, p. 88-96) :

2085. Le contrat de travail est celui par lequel une personne, le salarié, s'oblige, pour un temps limité et moyennant rémunération, à effectuer un travail sous la direction ou le contrôle d'une autre personne, l'employeur. (Code civil du Québec)

La **relation d'emploi** est essentiellement une relation d'échange dans laquelle l'employé contracte certaines obligations : l'exécution personnelle de son travail (ne pas le confier à

quelqu'un d'autre de sa propre initiative, sans en aviser son supérieur), l'obéissance, la prudence, la diligence, la loyauté, la discrétion, la non-concurrence. Pour sa part, l'employeur acquiert d'autres obligations : rémunérer selon le contrat et les lois applicables, fournir du travail selon le contrat, protéger l'intégrité et la dignité des personnes en vertu des droits fondamentaux (Gagnon, p. 104-135).

Comment définit-on la notion de **subordination juridique**? De nos jours, en raison de l'évolution du travail vers un accroissement de la complexité et des compétences (par opposition au travail à la chaîne, par exemple), on la définit de façon large. Il s'agit de la faculté qu'a l'employeur de déterminer le travail à exécuter, d'encadrer cette exécution et de la contrôler. Ce contrôle n'est pas forcément immédiat pour qu'il y ait subordination; il varie beaucoup selon le niveau de qualification et les emplois (Gagnon, p. 91-93).

Les limites qu'imposent les droits fondamentaux

Nous savons que l'employeur est en droit de contrôler et de surveiller la gestion, l'organisation et les finances de l'organisation de manière à s'assurer de son bon fonctionnement. Toutefois, il ne peut exercer ce droit selon sa seule discrétion; il doit l'exercer dans le respect des droits fondamentaux des salariés. Bien que l'employé ait consenti à une relation de subordination, en aucun cas il n'a consenti à l'abandon de la protection de ses droits fondamentaux, parmi lesquels figure le droit au respect de sa vie privée.

La Charte des droits et libertés de la personne protège le droit fondamental à la vie privée :

5. Toute personne a droit au respect de sa vie privée.

24.1. Nul ne peut faire l'objet de saisies, perquisitions ou fouilles abusives. (Charte des droits et libertés de la personne, LQ, chap. C-12).

Le droit à la vie privée n'est **pas absolu**, puisqu'il doit s'exercer dans le respect des lois et des valeurs démocratiques (Gingras et Gratton, 2014, p. 37) :

9.1. Les libertés et droits fondamentaux s'exercent dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec.

La loi peut, à cet égard, en fixer la portée et en aménager l'exercice. (Charte québécoise des droits et libertés de la personne).

Les gestes de l'employeur liés à la fouille, notamment les tests de dépistage, la surveillance électronique ou la fouille d'ordinateurs personnels, doivent se justifier par rapport l'article 9.1 de la charte québécoise, comme le précise un arrêt de la Cour suprême du Canada :

La partie qui invoque l'article 9.1 pour tenter de justifier la limitation d'un droit garanti par la charte québécoise a donc la charge de prouver que cette limite est imposée dans la poursuite d'un objectif légitime et important et qu'elle est proportionnelle à cet objectif, c'est-à-dire qu'elle est rationnellement liée à l'objectif et que l'atteinte au droit est minimale. (*Godbout c. Longueuil (ville de)* [1997] (CSC).

Le statut particulier des droits fondamentaux

Les **normes prééminentes** sont celles qui priment sur toutes les autres normes de rang inférieur. On y trouve, entre autres, la Charte canadienne des droits et libertés et la Charte des droits et libertés de la personne du Québec. Lorsque les normes ont ce statut, elles ont un pouvoir maximal.

On dit des lois qui énoncent les droits de la personne qu'elles sont des lois prééminentes en ce qu'elles s'imposent par leur **caractère constitutionnel** (la charte canadienne est incluse dans la Constitution canadienne, partie 1 de la Loi constitutionnelle de 1982 (annexe B de la Loi de 1982 sur le Canada (1982, RU, c. 11) ou **quasi constitutionnel**. À ce titre, tant les lois provinciales que fédérales doivent être conformes à la charte canadienne, à défaut de quoi elles peuvent être déclarées inconstitutionnelles et inopérantes. Les lois provinciales, à leur tour, doivent être conformes à la charte québécoise, à défaut de quoi elles peuvent aussi être déclarées inconstitutionnelles et inopérantes. Il en va de même des contrats et des conventions collectives.

Ces législations constitutionnelles (Charte canadienne des droits et libertés) ou quasi constitutionnelles (Charte des droits et libertés de la personne du Québec) s'imposent d'autorité sur toutes les autres lois et tous les contrats, y compris les conventions collectives, en cas de contradiction entre les dispositions des unes et des autres.

La **charte canadienne** régit les relations entre **l'État et ses sujets, mais non les relations des citoyens entre eux**. Elle établit un cadre auquel doit se conformer le législateur (le Parlement du Canada, les parlements provinciaux) en édictant les lois, en les exécutant (les ministères, la fonction publique) et en administrant la justice (les tribunaux judiciaires et administratifs).

En d'autres termes, une personne ne peut porter plainte contre une autre personne ni contre un employeur du secteur privé en vertu de la Charte canadienne des droits et libertés. En bref, la Charte s'applique :

- au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le Yukon et les Territoires du Nord-Ouest;
- à la législature et au gouvernement de chaque province, pour tous les domaines relevant de cette législature.

Dans le régime québécois, la situation est différente : le champ d'application de la Charte n'est pas restreint aux seuls domaines publics; **une personne peut porter une plainte contre une autre personne ou une entreprise en vertu de la charte québécoise**, car elle régit les rapports entre les citoyens.

Dans le régime canadien, la loi qui définit les droits des citoyens en divers domaines, et notamment du travail, établit les obligations découlant des droits fondamentaux garantis par la charte canadienne et permet à un individu lésé (sur le plan de l'emploi comme en tout autre domaine) de déposer des plaintes s'appelle la Loi canadienne sur les droits de la personne (LRC [1985] c. H-6), qui s'applique aux entreprises de compétence canadienne.



Rappel : Vous pouvez consulter les lois canadiennes et québécoises gratuitement dans Internet; vous trouverez facilement la version la plus récente au moyen de votre fureteur (voir les conseils plus haut). Il est important de lire attentivement les articles des lois cités dans cette synthèse. Lorsqu'un article est cité dans une décision de tribunal, lisez-le aussi. Cela est essentiel à votre bonne compréhension du raisonnement juridique.



Il importe avant tout de bien comprendre qu'il y a deux régimes juridiques applicables au Québec, selon la compétence à laquelle est assujéti l'employeur :

- Les organisations de compétence canadienne selon la Constitution canadienne sont celles qui ont leurs activités dans les secteurs économiques suivants :
 - le secteur bancaire;
 - les transports interprovinciaux;
 - les chemins de fer, canaux ou liaisons télégraphiques qui relient une province à une ou à plusieurs autres;
 - les communications par air ou par mer (transport routier interprovincial, navires, chemins de fer, canaux, avions, aéroports, traversiers, tunnels et ponts interprovinciaux);
 - les télécommunications (stations de radio et de télédiffusion, réseaux téléphoniques et télégraphiques, câblodistribution, postes);
 - les entreprises déclarées d'intérêt général pour le Canada et celles qui ne sont pas du ressort législatif des provinces (énergie nucléaire, extraction et traitement de l'uranium, pipelines, silos, élévateurs à grains autorisés par la Commission canadienne des grains, minoteries, usines de nettoyage des semences, exploration et mise en valeur des gisements de pétrole). Les salariés de l'État (fonctionnaires fédéraux) sont aussi régis par le régime juridique canadien plutôt que par celui des provinces où ils travaillent.

- Toutes les autres organisations sont de compétence québécoise. C'est le régime applicable à ces organisations que je présente dans ce chapitre.

Les lois sur la protection des renseignements personnels des employés

Notez qu'il n'existe pas **au Québec**, malgré cette erreur souvent entendue, de Loi sur l'accès à l'information. Au Québec, il n'existe qu'une Commission d'accès à l'information

(CAI). Il y a deux lois auxquelles on fait référence, selon les cas, et la CAI est l'organisme qui les administre. La première est la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels dans le secteur public (LRQ, c. A-2.1); je n'en parlerai pas ici. Je vais traiter davantage de cas relevant de la Loi sur la protection des renseignements personnels dans le secteur privé (LRQ, c. P-39.1).



Rappel : Vous pouvez consulter les lois canadiennes et québécoises gratuitement dans Internet; vous trouverez facilement la version la plus récente au moyen de votre navigateur (voir les conseils plus haut). Il est important de lire attentivement les articles des lois cités dans cette synthèse. Lorsqu'un article est cité dans une décision de tribunal, lisez-le aussi. Cela est essentiel à votre bonne compréhension du raisonnement juridique.

La Loi sur la protection des renseignements personnels dans le secteur privé

Selon cette loi, l'employeur ne peut pas librement recueillir ni utiliser des renseignements concernant ses employés. Les personnes visées doivent donner leur consentement à la collecte et à l'utilisation de renseignements personnels les concernant. Le consentement doit être explicite; en d'autres termes, on ne peut pas le déduire ou prétendre qu'il allait de soi :

14. Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Un consentement qui n'est pas donné conformément au premier alinéa est sans effet.
(Loi sur la protection des renseignements personnels dans le secteur privé)

Comme vous le verrez plus bas, il en va autrement dans le **droit de fouille**, où le consentement peut être explicite ou implicite.

Bien qu'un candidat ait donné son consentement pour la collecte et l'utilisation de renseignements personnels le concernant, l'employeur doit remplir certains critères précis afin de constituer un dossier. Selon la Loi sur la protection des renseignements personnels dans le secteur privé, l'employeur doit avoir un intérêt sérieux et légitime pour constituer un dossier sur un candidat :

4. Toute personne qui exploite une entreprise et qui, en raison d'un intérêt sérieux et légitime, peut constituer un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet.

Cette inscription fait partie du dossier.

5. La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires à l'objet du dossier.

Ces renseignements doivent être recueillis par des moyens licites.

La personne visée doit être informée de la collecte d'informations la concernant, mais l'employeur peut en transmettre certaines sans son consentement, dans des cadres précis :

8. La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer :

1° de l'objet du dossier;

2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;

3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification.

18. Une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui :

[...]

4° à une personne à qui il est nécessaire de communiquer le renseignement dans le cadre d'une loi applicable au Québec ou pour l'application d'une convention collective;

[...]

6° à une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions.

Les lois fédérales

Pour votre usage personnel, mentionnons trois lois de compétence canadienne, qu'il ne faut pas confondre avec les lois québécoises :

- la Loi sur l'accès à l'information (LR, 1985, chap. A-1), qui vise le droit d'accès des individus aux documents détenus par les institutions fédérales;
- la Loi sur la protection des renseignements personnels (LR, 1985, chap. P-21), qui vise à responsabiliser quelque 150 ministères et organismes fédéraux quant au respect des droits à la vie privée des individus en limitant la collecte, l'utilisation et la communication des renseignements personnels et qui confère aux personnes concernées le droit d'accès aux renseignements personnels détenus à leur sujet par ces institutions fédérales et organismes désignés;
- la Loi sur la protection des renseignements personnels et les documents électroniques (2000, chap. 5), qui s'applique aux entreprises de compétence canadienne comme les banques, les compagnies de chemin de fer, les compagnies de transport aérien ou interprovincial et qui prévoit des règles régissant la collecte, l'utilisation, la communication des renseignements personnels dans le cadre d'activités commerciales et l'accès à ces informations.



Rappel : Vous pouvez consulter les lois canadiennes et québécoises gratuitement dans Internet; vous trouverez facilement la version la plus récente au moyen de votre fureteur (voir les conseils plus haut). Il est important de lire attentivement les articles des lois cités dans cette synthèse. Lorsqu'un article est cité dans une décision de tribunal, lisez-le aussi. Cela est essentiel à votre bonne compréhension du raisonnement juridique.

LE PROBLÈME VISÉ

Le contenu des appareils électroniques, la vie privée et les intérêts de l'employeur

L'employeur peut avoir des motifs fondés de soupçonner divers délits : un employé enregistre des collègues à leur insu, installe des logiciels sans autorisation, envoie des logiciels piratés à des connaissances, utilise Internet de façon indue pendant les heures de travail et « vole du temps », fraude l'organisation, et ainsi de suite.

La **concurrence déloyale** est l'un de ces délits dont il est question dans ce cours (voir à ce sujet la synthèse de la doctrine sur les ententes restrictives). Ce délit prend notamment la forme d'un employé qui nourrit des projets contraires aux intérêts de l'entreprise, met sur pied une entreprise concurrente pendant qu'il est en relation d'emploi avec un employeur, utilise l'ordinateur fourni pour la gestion d'une entreprise personnelle. Il enfreint ainsi son devoir de loyauté envers l'employeur. Il le fait parfois pendant ses heures de travail ou à partir des ordinateurs, des portables, des téléphones intelligents et d'autres appareils sans fil fournis par l'employeur pour exercer ses fonctions. Ce phénomène soulève aujourd'hui des questions importantes sur la protection de la vie privée à l'occasion du travail.

L'employeur a le droit, en vertu de ses droits de direction et à **certaines conditions** (que nous allons voir plus bas), de mener des enquêtes sur des comportements qu'il croit fautifs lorsque ceux-ci se produisent sur les lieux et pendant les heures de travail. L'employeur n'espionne pas alors un salarié dans les activités de sa vie privée, mais vérifie s'il effectue le travail pour lequel il le paye, travail qui exige l'utilisation d'un ordinateur.

Qu'en est-il de l'accès au réseau Internet, de l'adresse électronique, du courriel et des échanges dans les réseaux sociaux en contexte d'emploi? Relèvent-ils de la vie privée? Les fichiers consultés et les courriels envoyés et reçus sont emmagasinés sur un disque dur. Sont-ils protégés de la fouille par l'employeur par le droit à la vie privée?

L'employé **conserve son droit à la protection de la vie privée** au travail, mais celui-ci est **limité en contexte d'emploi**. L'employeur peut instaurer une politique, des mesures et des directives relatives à l'utilisation des outils électroniques. Il peut préciser que l'usage des

courriels et d'Internet est strictement interdit à des fins personnelles. Un employé a le devoir de ne pas en faire un usage personnel déraisonnable.

Il peut aussi arriver que l'employeur découvre un comportement délinquant d'un employé de façon fortuite, par exemple à l'occasion de l'entretien routinier du réseau par un technicien (arrêt *R. c. Cole* [2012] (CSC)).



Si vous le souhaitez et pour satisfaire votre curiosité seulement, lisez à ce sujet les décisions *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (CSN) c. Trudeau* [1999] (CA) et *R. c. Cole* [2012] (CSC), fournies dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques ».

Dans certains contextes, l'employeur pourra consulter les courriels d'un employé au travail à son insu, sans que le tribunal considère qu'il y a atteinte au droit à la vie privée de l'intéressé (cas illustré, par exemple, dans la décision *Université Laval et Association du personnel administratif professionnel de l'Université Laval (APAPUL)* [2011] (TA)). L'employeur doit néanmoins faire usage de ce droit avec précaution car, en cas de litige, il aura le fardeau de prouver qu'il avait des motifs raisonnables d'intercepter ou de consulter les courriels de son employé.

À cet égard, le tribunal doit exercer, dans chaque cas, un arbitrage entre les droits à la vie privée des salariés et les droits de la direction. Le tribunal, en cas de plainte, a pour tâche de réconcilier l'usage des technologies de l'information en contexte d'emploi et la protection de la vie privée au travail. Il étudie chaque cas en contexte.

Pour établir qu'il y a atteinte à la vie privée, on va considérer : la nature des communications surveillées, la propriété des outils informatiques, la nature du travail exercé par l'employé, la tolérance de l'employeur relativement à l'utilisation d'Internet ou du courriel à des fins personnelles, **l'existence d'une politique** concernant les technologies de l'information, etc. Chaque cas demeure un cas d'espèce.

Le droit à la vie privée inclut-il la protection des renseignements personnels emmagasinés dans un ordinateur *personnel*?

La Cour suprême (dans la décision *R. c. Vu* [2013] (CSC)), a établi quatre catégories d'informations que peut emmagasiner un ordinateur ou auxquelles on peut accéder par celui-ci :

- 1.- les informations emmagasinées dans le disque dur de l'ordinateur par l'utilisateur, consultables dès que l'ordinateur est en fonction, qu'il soit ou non connecté à Internet et que la barrière de protection, comme le mot de passe, a été franchie, à l'aide des logiciels installés sur l'ordinateur et appropriés au format du fichier; certaines, notamment

- dans le cas des ordinateurs personnels, portent sur l'ensemble des renseignements biographiques d'ordre personnel;
- 2.- les informations générées automatiquement par l'ordinateur et emmagasinées dans celui-ci :
 - a) les métadonnées (données à propos ou décrivant d'autres données) qui peuvent permettre de retracer l'historique d'un fichier ou de déterminer la date à laquelle un fichier a été créé ou modifié, les dates où l'employé a accédé à de l'information confidentielle (par exemple, après la fin de son emploi), le fait qu'il a copié une partie de cette information sur des clés USB, le temps passé à naviguer dans Internet ou la date où une photo a été prise;
 - et b) l'historique de navigation sur Internet, les pages Web visitées, les recherches effectuées, incluant la mémoire cache; si l'utilisateur l'a autorisé, les navigateurs peuvent conserver les mots de passe des services en ligne et les informations des formulaires Web; d'autres informations relatives, entre autres, à la navigation sur Internet et à la transmission et la réception de courriels sont aussi susceptibles d'être emmagasinées non pas sur l'ordinateur de l'employé, mais plutôt sur les serveurs de l'employeur;
 - 3.- les informations emmagasinées dans l'ordinateur, mais qui ont été effacées par l'utilisateur; même si l'utilisateur a supprimé la corbeille ou l'historique de navigation, l'ordinateur ne les fait toutefois pas disparaître entièrement tout de suite; par ailleurs, lorsqu'une information diffusée par l'entremise d'un service en ligne, tels Facebook, Twitter ou Snapchat, ne sera plus accessible via le compte de l'utilisateur, il pourra aussi, dans certains cas, être possible d'obtenir l'information par l'entremise dudit service en ligne;
 - 4.- les informations non emmagasinées dans l'ordinateur, mais accessibles par celui-ci. Les ordinateurs peuvent, par l'entremise d'un navigateur Web, être utilisés pour accéder à des informations qui ne sont pas emmagasinées dans l'ordinateur lui-même, mais plutôt emmagasinées dans l'infonuagique; de même, un ordinateur connecté à un réseau permettra à la police d'avoir accès à des renseignements se trouvant dans d'autres appareils. Par conséquent, la fouille d'un ordinateur connecté à Internet ou à un réseau permet d'avoir accès à des données et à des documents qui ne se trouvent pas concrètement dans le lieu où la fouille est autorisée. Lorsque l'utilisateur aura sauvegardé dans l'ordinateur, par l'entremise du navigateur Web, les noms d'utilisateur et les mots de passe lui permettant d'accéder à ses comptes de services en ligne, il sera loisible à tout individu utilisant ce même ordinateur, d'accéder à ces comptes, de prendre connaissance de l'information diffusée par l'entremise de ceux-ci et d'usurper l'identité du titulaire du compte (Gingras et Gratton, 2014, p. 40-50, citant la décision *R. c. Vu* [2013] (CSC)).

En tenant compte de ces éléments de définition, il est possible d'affirmer que les informations emmagasinées **dans un ordinateur personnel, y compris une tablette et un**

téléphone intelligent (selon la Cour suprême dans l'arrêt *R. c. Vu* [2013] (CSC)), font partie de la **vie privée de son utilisateur**. Le terme « ordinateur » peut, en effet, comprendre les ordinateurs, les tablettes et les téléphones intelligents (Gingras et Gratton, 2014, p. 36).

Lorsque cette information est emmagasinée dans un ordinateur **personnel**, le droit à la vie privée de son utilisateur est reconnu et les risques d'atteinte à la vie privée sont réduits. Toutefois, lorsqu'un **ordinateur professionnel est aussi utilisé à des fins personnelles**, ou qu'un **ordinateur personnel est utilisé à des fins professionnelles**, les outils de communication électronique fournis par l'employeur posent un défi de taille à la protection du droit à la vie privée, dans le contexte du droit de fouille de l'employeur que nous verrons plus bas :

En milieu de travail, il est raisonnable de s'attendre que l'employeur contrôle l'utilisation des moyens de communication qui lui appartiennent. Toutefois, l'employé a droit au respect de sa vie privée dans l'exercice de ce contrôle. Les employés doivent ainsi être informés des motifs de contrôle et des mécanismes de contrôle dont ils peuvent être l'objet. Ils doivent être clairement informés de leurs obligations et de leurs droits. (CAIQ, p. 5)

Les enjeux liés au contenu de ces appareils sont de plus en plus importants en matière de protection de la vie privée :

De nos jours, les ordinateurs font partie intégrante de nos vies, tant personnelles que professionnelles, et peuvent emmagasiner une quantité phénoménale d'informations, dont des courriels, incluant tant ceux envoyés que reçus, l'historique de consultation des sites Internet, un agenda, des documents, de nature médicale et financière, des photographies et des vidéos, de même que des documents téléchargés, numérisés et sauvegardés (*R. c. Morelli* [2010] (CSC), parag. 3). Ces informations se situent bien souvent au cœur même de l'ensemble des renseignements biographiques d'une personne (*R. c. Morelli* [2010] (CSC), parag. 48).

Il est souvent possible, lorsque le nom d'utilisateur et le mot de passe d'un service en ligne, tel que Hotmail, Facebook ou Dropbox, sont enregistrés par défaut dans un ordinateur, d'accéder par l'entremise de cet ordinateur aux informations diffusées par le biais de ces services et emmagasinées, non pas sur l'ordinateur lui-même, mais sur les serveurs des entreprises qui gèrent ces services en ligne. (Gingras et Gratton, 2014, p. 36)

Ces informations s'accroissent lorsque l'ordinateur est aussi utilisé pour naviguer sur Internet puisque les informations susceptibles d'être emmagasinées dans l'historique de navigation et la mémoire cache du navigateur Web (navigateur) peuvent aussi permettre de connaître les intérêts particuliers, préférences et propensions de l'utilisateur à la lumière des recherches effectuées et des sites consultés. Ces informations constituent un instrument aux multiples facettes sans précédent dans notre société et soulèvent, en matière de protection de la vie privée, des préoccupations particulières dont les tribunaux doivent tenir compte lorsque vient le moment d'admettre une preuve de cette nature. (Gingras et Gratton, 2014, p. 40)

L'employé qui estime que l'employeur commet une intrusion injustifiée dans sa vie privée, par exemple parce qu'il surveille ses activités dans Internet ou ses courriels, a des recours. Les employés les exercent de plus en plus (Gingras et Gratton, 2014, p. 38).

Avant de considérer les recours de l'employé en cas de contravention au droit à la vie privée, il faut connaître les obligations qui s'imposent d'office à lui en vertu du droit québécois.

Une obligation qui restreint le droit à la vie privée de l'employé : le devoir de loyauté

Le **devoir de loyauté** est énoncé aux articles 2088-2089 CcQ et impose à tout salarié, peu importe son poste ou son niveau hiérarchique, d'agir avec loyauté et bonne foi envers son employeur. En pratique, cela signifie que comme un salarié ne travaille pas pour son propre compte, mais qu'il met sa force de travail à la disposition d'un employeur qui dispose des fruits de son travail, il doit :

- dans le cadre du travail, promouvoir et faire primer les intérêts de l'employeur sur les siens;
- se conduire avec honnêteté envers l'employeur : éviter de mentir, de voler, de frauder, s'approprier les biens de son employeur ou en détourner l'usage à des fins personnelles;
- éviter de saboter ou d'entraver l'entreprise qui l'embauche,
- éviter de se placer en conflit d'intérêts et de privilégier ses propres intérêts ou ceux de tiers au détriment de ceux de son employeur;
- respecter et préserver la confidentialité de certains renseignements dont il prend connaissance à l'occasion de son travail; le **devoir de discrétion** est **illimité** à l'endroit des **renseignements personnels** concernant l'employeur, les collègues, les clients, les tiers, la réputation et la vie privée d'autrui (art. 2088(2) CcQ);
- par déduction, **ne pas faire concurrence à son employeur** pendant la durée de son emploi (Bich, 2003, p. 253-254).

Pour qu'il y ait **conflit d'intérêts**, il n'est pas nécessaire que le salarié accomplisse une action malhonnête ou favorise dans les faits ses intérêts (ou ceux d'un tiers) au détriment de ceux de son employeur. Il suffit qu'il se trouve dans la situation où il pourrait le faire (bien entendu, l'employeur devra faire preuve de mesure et de prudence dans l'appréciation d'une telle situation). De la même façon, un salarié ne saurait concurrencer son employeur en exploitant son propre commerce ou sa propre entreprise hors des heures de travail (dans ce cours, une autre synthèse de la jurisprudence porte sur cet objet).

Quel est le pouvoir de fouille de l'employeur qui soupçonne une rupture de l'obligation de loyauté?

La question de la fouille des appareils fournis aux employés peut se poser quand l'employeur cherche à découvrir et à obtenir des éléments de preuve concernant un employé actuel ou ancien soupçonné de concurrence déloyale ou de planifier une violation d'une clause de non-concurrence. L'employeur aux prises avec un soupçon de concurrence

déloyale peut saisir et fouiller l'ordinateur portable de son employé quand il a des motifs de croire que l'employé en cours d'emploi planifie une concurrence déloyale ou quand il soupçonne la concurrence déloyale d'un employé déjà parti (Monet, 2013, p. 55). Il cherche à rassembler les preuves nécessaires au succès de sa démarche judiciaire pour empêcher la concurrence déloyale ou la violation de l'entente de non-concurrence.

Dans le rassemblement des éléments de preuve, l'ordinateur de l'employé peut être une importante source de preuve : échange de courriels, rendez-vous, personnes-ressources et sites Internet visités. Même si l'employé détruit les traces de ses actes, des services spécialisés à des fins d'enquête (tel *eDiscovery*) peuvent récupérer des éléments supprimés et reconstituer, par exemple, une boîte de réception (Monet, 2013, p. 52).

QUEL EST LE RECOURS DE L'EMPLOYEUR LÉSÉ?

Nous avons vu que l'employeur peut s'estimer lésé parce qu'un ex-employé contrevient à son devoir de loyauté en vertu de l'article 2088 CcQ, par exemple à l'obligation de ne pas faire concurrence à son employeur ou d'une autre façon.

L'employeur peut alors exercer deux recours :

- Il peut demander au tribunal d'ordonner une **injonction – permanente** ou **temporaire (interlocutoire)** – permettant un résultat rapide lorsque le besoin est urgent, car si le tribunal l'ordonne, l'injonction prend effet immédiatement. L'injonction tente d'empêcher un comportement à venir, lorsqu'on a de bonnes raisons de croire qu'il se produira.
- L'employeur peut aussi demander des **dommages et intérêts**, soit la réparation des dommages subis par une compensation matérielle de la personne fautive (Launay et Dufresne, 2008, p. 241). Les dommages sanctionnent souvent un comportement passé, par exemple lorsqu'il est trop tard et que le tort est fait (Lemoine et Courchesne Tardif, 2011, p. 199). Cependant, la jurisprudence permet aussi de compenser un *préjudice futur*, si une partie lésée parvient à démontrer qu'il est hautement probable, plus qu'hypothétique et qu'il a un caractère de *certitude raisonnable* (Lemoine et Courchesne Tardif, 2011, p. 214-218).

Le tribunal à qui on soumet un recours pour une telle contravention cherche à vérifier :

- si l'obligation de loyauté qu'invoque l'employeur s'applique et si, telle qu'invoquée, elle est raisonnable,
- si la contravention a bien eu lieu, sa confirmation,
- si le préjudice que l'employeur dit subir est aussi confirmé,
- si la réparation recherchée (ordonnance d'injonction ou somme des dommages) est proportionnelle au préjudice.

Depuis l'entrée en vigueur du nouveau Code civil en 1994, le législateur a inversé le fardeau de la preuve dans le cas des recours pour manquement au devoir de loyauté. **L'employeur a le fardeau de démontrer** le fait qu'il y a eu manquement (art. 2089(3) CcQ; Bich, 2003, p. 256). Le législateur a pris cette décision à cause de la dissymétrie des rapports de pouvoir entre employeurs et employés (Béliveau et Lebel, 2011, p. 126).

L'ordonnance d'injonction

L'**injonction** est un recours extraordinaire qui ne peut être accordé au Québec que par la Cour supérieure. La Cour supérieure ordonne par ce recours à une personne, à ses dirigeants, représentants ou employés, de ne pas faire ou de cesser de faire, ou, dans les cas qui le permettent, d'accomplir un acte ou une opération déterminés, sous la menace des peines que prévoit le droit (art. 751 Cpc).

L'employeur lésé peut demander l'exécution forcée de l'obligation elle-même sous l'autorité de la justice par une **ordonnance d'injonction**; en d'autres termes, il demande au tribunal de forcer l'employé sortant à respecter son obligation :

- soit en faisant quelque chose, en général respecter, exécuter ses obligations,
- soit en cessant de faire quelque chose, par exemple un comportement interdit en matière de concurrence (Lemoine et Courchesne Tardif, 2011, p. 199).

Les choses que l'employeur demande de faire ou de cesser de faire doivent être formulées clairement, précisément, sans ambiguïté, et la personne à qui on ordonne (de faire ou de cesser de faire) ne doit pas interpréter ou faire interpréter par un expert ses obligations. Elles doivent être **claires, simples, exécutoires** sans requérir d'avis juridique. L'ordonnance doit être raisonnable et se limiter à maintenir la situation préexistante ou à faire respecter une entente conclue, par exemple, et non à améliorer la situation préexistante ou à fournir davantage que ne le prévoit l'entente conclue.

À défaut d'être claire et raisonnable, l'ordonnance peut rester lettre morte, et l'employeur lésé doit alors déposer un autre recours en outrage au tribunal. Ce dernier recours peut lui-même échouer parce que l'ordonnance telle que rédigée est trop floue.

La question de l'urgence dans les cas de concurrence déloyale

Les tribunaux sont souvent sollicités pour agir d'urgence pour prévenir un préjudice irréparable à l'employeur. Il faut réagir vite dans les situations de concurrence déloyale ou de violation alléguée d'une entente de non-concurrence (pour en savoir plus, lisez la synthèse de la doctrine sur les ententes restrictives). L'employeur doit alors rapidement préparer un dossier étoffé pour convaincre un juge de la Cour supérieure de rendre une première ordonnance temporaire qui suspend les activités de l'employé soupçonné.

Dans la plupart des cas, l'employé met en place la concurrence pendant qu'il est toujours en relation d'emploi : assemblage d'informations confidentielles, consultation de données financières, communications avec les fournisseurs et la clientèle, tentative discrète d'intéresser d'autres employés à le rejoindre, etc. S'ils ne sont pas liés par une entente de non-concurrence, c'est à ce moment qu'ils peuvent faire l'objet d'une injonction. L'employeur doit agir vite.

Lorsqu'un client desservi par l'employeur a déjà manifesté son intérêt pour l'entreprise concurrente en formation, les employés en concurrence déloyale pourront s'engager dans leur entreprise à brève échéance. Les tribunaux tendent à imposer un court délai de répit à l'ex-employeur (pendant lequel l'ex-employé doit s'abstenir de faire concurrence à son ex-employeur). Si l'ex-employeur veut en bénéficier, il doit saisir les tribunaux aussitôt que possible lorsqu'il soupçonne le fait.

Comment l'employeur peut-il obtenir les preuves dans les délais nécessaires sans pouvoir saisir et fouiller les appareils électroniques? (Monet, 2013, p. 62).

Outre l'**injonction**, une partie peut, au début ou au cours d'une instance, obtenir une **injonction interlocutoire**. L'**injonction interlocutoire** peut être accordée en cas d'urgence, lorsque celui qui la demande paraît y avoir droit et qu'elle est jugée nécessaire pour empêcher que ne lui soit causé un préjudice sérieux ou irréparable, ou que ne soit créé un état de fait ou de droit de nature à rendre le jugement final inefficace (art. 752 Cpc).-La demande d'injonction interlocutoire est faite au tribunal par requête écrite appuyée d'un *affidavit* attestant la vérité des faits allégués et signifiés à la partie adverse, avec un avis du jour où elle sera présentée. Dans les cas d'extrême urgence, un juge peut toutefois y faire droit provisoirement, même avant qu'elle n'ait été signifiée. L'audience est plus rapide, mais une injonction **interlocutoire provisoire** ne peut en aucun cas, sauf dans le cas du consentement des parties, excéder 10 jours (art. 753 Cpc).

Les principes régissant l'émission d'une ordonnance d'injonction interlocutoire sont exprimés au mieux par le juge Owen, de la Cour d'appel, dans le désormais célèbre arrêt *Société de développement de la Baie James c. Kanatewat* [1975] (CA). Bien qu'il remonte à plus de 30 ans, cet arrêt résume bien tous les principes de droit applicables encore aujourd'hui à l'injonction interlocutoire, comme en fait foi l'extrait de la décision suivante :

L'art. 752 Cpc, écrit-il, impose au requérant en injonction interlocutoire de réussir deux tests ou de surmonter deux obstacles successifs. D'abord, il lui faut convaincre le tribunal qu'il **paraît avoir droit à l'injonction**, c'est-à-dire que le droit sur lequel il s'appuie a des chances raisonnables d'être reconnu par le jugement final. Dans une deuxième étape, s'il franchit avec succès ce premier test, le requérant devra démontrer l'**existence de circonstances exceptionnelles** faisant en sorte que l'injonction interlocutoire s'avère nécessaire pour lui éviter soit un **préjudice sérieux ou irréparable**, soit une situation de fait ou de droit de nature à rendre le jugement final

inefficace. (*Transports médicaux TRÈS c. Corporation de transport adapté « La roue de vie »* [2006] (CS), parag. 12)

Au stade de l'injonction interlocutoire, le tribunal agit très vite dans une situation d'urgence où l'on doit limiter les dommages; le tribunal doit donc juger les faits très rapidement et prendre une décision en l'absence d'un examen en profondeur. Il doit évaluer si quatre conditions importantes sont remplies :

- Le fardeau de preuve qu'on lui demande est allégé : si la contravention que reproche l'employeur est de l'ordre de la concurrence déloyale, le tribunal s'assure que **l'entente de non-concurrence conclue est raisonnable** et que le congédiement a été imposé pour un **motif sérieux** (Launay et Dufresne, 2008, p. 241).
- Il se limite ensuite à constater **l'apparence de droit**, c'est-à-dire que le moyen invoqué n'a qu'à être suffisamment sérieux pour offrir une perspective raisonnable de succès quand l'affaire sera plaidée au fond. À l'inverse, si la clause de non-concurrence est manifestement déraisonnable, il y a **absence d'apparence de droit** et l'analyse s'arrête là (illustré, par exemple, dans la décision *GS/C Communication inc. c. Maurice* [2007] (CS), parag. 22).
- L'employeur est menacé d'un **préjudice sérieux ou irréparable** si la situation continue.
- Il y a **urgence d'agir**.
- Lorsqu'on compare les **inconvenients** subis par les deux parties, **l'employeur en subit davantage** (*balance of convenience and inconvenience*) (Launay et Dufresne, 2008, p. 241; Laurier et Tremblay, 2013, p. 37).

Dans les cas où il semble clair que les requérants détiennent bien les droits qu'ils invoquent, **l'injonction** sera émise si le tribunal la considère nécessaire. En revanche, si l'existence des droits invoqués à ce stade paraît douteuse, le tribunal devra apprécier le poids relatif des inconvenients pour décider si l'injonction devrait ou non être accordée. Enfin, s'il apparaît, toujours à ce stade, que les droits invoqués sont inexistantes, alors l'injonction interlocutoire devra être refusée.

Le tribunal demande essentiellement, pour accorder l'ordonnance, qu'il y ait un risque réel de destruction (ou de disparition) de documents ou de biens pouvant servir de preuve et qu'on précise les éléments de preuve recherchés; en d'autres termes, qu'il ne s'agisse pas « d'aller à la pêche » (Monet, 2013, p. 65).

Dans certains cas, cependant, l'employeur n'a pas d'autre choix que de fouiller largement, parce qu'il est impossible de cibler les données pertinentes à saisir, étant donné le volume de données que contient un ordinateur. Dans un cas inusité, un employé de haut rang (directeur scientifique) s'est adonné à une concurrence parallèle durant sept ans, en contravention d'engagements de non-concurrence et de non-sollicitation signés en raison de l'importance stratégique de son poste (*AriVac inc. c. Achacha* [2012] (CS)). Il a utilisé le

laboratoire de l'entreprise, ses techniciens, ses procédés et ses technologies afin de réaliser des projets rémunérés, au nom de sa propre entreprise. L'employeur lésé a obtenu du tribunal une ordonnance afin d'autoriser des huissiers et un expert en informatique à rechercher, sur les disques durs des ordinateurs, logiciels, accessoires, supports informatiques et filières personnelles de l'ex-directeur, de même qu'au lieu de résidence (de manière plus restreinte), toute information se rapportant à ses propriétés intellectuelles et aux contrats que lui et son entreprise auraient exécutés en contravention des engagements de non-concurrence, de non-sollicitation, de non-utilisation, de loyauté et d'exclusivité applicables (Monet, 2013, p. 64).

Le recours en dommages-intérêts

L'employeur lésé peut demander la compensation du préjudice subi à la suite d'une contravention à une obligation par le versement d'une somme d'argent qu'on appelle des *dommages*.

Le **préjudice** peut consister en :

- une perte subie, même si elle consiste en la privation d'une possibilité, ou
- un gain dont on est ou sera privé.

Dans les deux cas, la preuve de la valeur des dommages subis peut être difficile à faire, notamment la perte de clientèle, que les tribunaux affirment souvent difficile à estimer (Lemoine et Courchesne Tardif, 2011, p. 200). Par exemple, l'employeur doit démontrer que n'eût été du comportement délinquant de son ex-employé en matière de concurrence, il aurait probablement profité de l'occasion d'affaires X dont il a été privé, ou alors il aurait obtenu l'avantage qu'a indûment obtenu l'ex-employé (Lemoine et Courchesne Tardif, 2011, p. 213).

Enfin, le préjudice peut consister en un gain réalisé par le contrevenant parce qu'il a contrevenu à son obligation. En effet, le tribunal considère qu'il serait inacceptable que la partie en faute tire avantage de son geste fautif sans devoir indemniser l'entreprise dont elle envahit le marché et envers laquelle elle a une obligation (Lemoine et Courchesne Tardif, 2011, p. 212-216, citant la décision *Uni-Sélect inc. c. Aktion corp.* [2002] (CA)).

Ce dernier recours est plus exigeant. L'employeur doit prouver :

- l'ampleur de la perte subie, du gain manqué; par exemple, le prix d'un contrat perdu, le prix du marché pour des biens invendus, la marge habituelle de profit perdue à cause d'une concurrence déloyale (Lemoine et Courchesne Tardif, 2011, p. 214);
- la violation par l'employé des obligations contenues dans l'entente (Launay et Dufresne, 2008, p. 242);

- le lien causal entre l'inexécution par l'ex-employé de l'obligation et le préjudice subi (Lemoine et Courchesne Tardif, 2011, p. 214).

LE RECOURS DE L'EMPLOYÉ LÉSÉ

Contester l'admissibilité d'une preuve

L'employé peut-il contester l'**admissibilité d'une preuve** obtenue par l'employeur au moyen d'une saisie et d'une fouille du contenu d'un ordinateur fourni comme outil de travail? Lorsqu'un employeur a procédé à une fouille qui ne respecte pas ses droits fondamentaux, l'ex-employé peut-il demander des dommages pour atteinte à la vie privée?

Compte tenu du volume de fichiers, de renseignements et d'images qui peuvent se trouver dans un ordinateur et de l'expansion des frontières de la recherche pour atteindre un ordinateur personnel, il est prévisible que le tri effectué par un employeur du matériel accessible lui dévoile une foule de renseignements sur son employé ou ex-employé qui relèvent strictement de sa vie privée et qui n'ont aucune pertinence par rapport à la concurrence déloyale. Il est pratiquement inévitable que des éléments subjectifs liés à la personnalité de ce dernier soient exposés et qu'il y ait atteinte à la vie privée. Les tribunaux prennent en compte la nature des renseignements et des informations que l'employeur saisit et examine, afin de trancher s'il y a atteinte à la vie privée. Les courriels de nature privée ne peuvent être **admis comme preuve** (Monet, 2013, p. 73).

En revanche, dès que les renseignements portent sur l'employeur ou relèvent de la planification d'une concurrence d'affaires par l'employé, ils ne relèvent plus de la vie privée de l'employé, mais bien des obligations du contrat de travail (Monet, 2013, p. 74).

Contester l'atteinte à la vie privée

Lorsque l'employeur a enquêté sur un employé et est parvenu à démontrer qu'il s'est rendu coupable de concurrence déloyale, l'employé peut contester l'atteinte à la vie privée. **Même lorsqu'il est coupable** de concurrence déloyale, l'employé peut obtenir des dommages pour atteinte à la vie privée; cela n'est pas exclu.

LE DROIT DE FOUILLE EN CONTEXTE D'EMPLOI

Le droit de fouille de l'employeur et le droit à la vie privée

Plusieurs actions accomplies par l'employeur sont régies par le droit sur les fouilles : les examens médicaux avant l'embauche et pendant l'emploi qui comportent des prélèvements, les tests de dépistage de l'intoxication, la surveillance électronique par caméra vidéo sur les

lieux de travail ou hors du travail en cas de congé de maladie, la fouille d'ordinateurs personnels, notamment (Pedneault, Bernier et Granosik, 2015, p. 17-2).

En principe, on ne peut fouiller dans les éléments de la vie privée d'une personne sans son **consentement**, sous réserve de l'application des lois et des situations qui permettent de le faire dans certaines circonstances particulières. En effet :

Le droit à la vie privée, par contre, n'est pas absolu. Il est balisé par une série de limites et sa mise en œuvre appelle un équilibre avec d'autres droits fondamentaux, dont le droit du public à l'information. On ne pourrait donc qualifier d'illicite ou fautive la violation du droit à la vie privée, s'il existe une justification raisonnable, une fin légitime ou encore si l'on peut conclure au consentement par la personne à l'intrusion dans sa vie privée. (décision *The Gazette c. Valiquette* [1996] (CA))

La fouille est une **atteinte à la vie privée** (Pedneault, Bernier et Granosik, 2015, p. 21-1 et 21-3) et, dans ce contexte, l'employeur peut, dans certains cas, contrevenir à la vie privée de ses employés. Dans le cas des enquêtes publiques, il est interdit de fouiller sans autorisation judiciaire préalable.

Cependant, l'employeur a le droit de protéger ses biens, tant que les mesures pour ce faire ne sont pas discriminatoires ou abusives. L'employeur a des **intérêts légitimes** à protéger : la sécurité des lieux de travail, ses biens et sa propriété. Pour cette raison, l'employeur a le droit de fouiller ses employés, parce que l'enquête est ici de nature privée (Pedneault, Bernier et Granosik, 2015, p. 21-3 et 21-4).

Tant des lois que de la jurisprudence, il ressort que pour restreindre l'intégrité de la personne et compromettre son droit à la vie privée, il faut pouvoir invoquer le **consentement** libre, volontaire et éclairé (art. 10 et 1399 CcQ) du salarié (au moment de la demande d'emploi, dans le contrat individuel de travail) :

10. Toute personne est inviolable et a droit à son intégrité.

Sauf dans les cas prévus par la loi, nul ne peut lui porter atteinte sans son consentement libre et éclairé.

1399. Le consentement doit être libre et éclairé.

Il peut être vicié par l'erreur, la crainte ou la lésion.

Cependant, l'employeur peut aussi invoquer des **circonstances exceptionnelles**. Par exemple, on peut violer le droit à la vie privée s'il existe une **justification raisonnable** ou encore si l'on peut **déduire le consentement** du contexte par la personne à l'intrusion dans sa vie privée (*The Gazette c. Valiquette* [1996] (CA)).

Par exemple, les employeurs ont un pouvoir de surveillance et de contrôle en vertu de la relation de subordination (art. 2085 CcQ); on peut en déduire le droit de l'employeur de vérifier les informations emmagasinées dans un ordinateur, ainsi que l'utilisation de celui-ci

par un employé, droit que les tribunaux ont à maintes reprises reconnu aux employeurs (Gingras et Gratton, 2014, p. 37).

Toutefois, cette vérification ne doit en aucun cas être arbitraire ou discriminatoire. Cela ne donne pas carte blanche aux employeurs afin d'espionner leurs employés dans leur vie privée et ne confère pas le droit à des utilisations abusives. Toute intrusion de l'employeur dans la vie privée de l'employé doit être justifiée par des **motifs rationnels, sérieux et fondés** et conduite par des **moyens raisonnables et proportionnels**, de façon à porter le moins possible atteinte au droit à la vie privée de l'employé (lire à ce sujet *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (CSN) c. Trudeau* [1999] (CA); Gingras et Gratton, 2014, p. 38).

L'employeur peut aussi souhaiter vérifier les affirmations d'un travailleur soupçonné de déloyauté (ou encore absent pour maladie), à condition d'avoir des raisons sérieuses de le faire, et avoir recours pour le faire à des firmes de filature et de surveillance vidéo. Lorsque le travailleur est à l'extérieur de chez lui, sur son terrain ou dans l'espace public, l'attente de vie privée est moins grande, de même que la protection (Pedneault, Bernier et Granosik, 2015, p. 22-13). Dans ce cadre, seuls les abus sont condamnés, soit en vertu de la durée de la surveillance, soit en vertu de son intensité ou de sa constance.

Le droit de fouille des appareils informatiques

La fouille de ces appareils n'a aucune commune mesure avec celle d'autres contenants se trouvant habituellement dans les lieux de travail, tel un classeur se trouvant dans un bureau et appartenant clairement à l'employeur (Gingras et Gratton, 2014, p. 37, citant l'arrêt *R. c. Vu* [2013] (CSC)). Dans quelles situations un employeur peut-il accéder à l'information emmagasinée dans un tel ordinateur?

À ce sujet, il faut respecter les principes généraux du droit sur les fouilles (vus plus haut). Plus les motifs de l'employeur sont **rationnels, fondés et sérieux**, plus on lui reconnaît un intérêt à vérifier l'information emmagasinée dans l'ordinateur d'un employé. Le raisonnement du tribunal dans ces cas consiste à se demander si une personne raisonnable, se trouvant dans la même situation, **s'attendrait à ce que sa vie privée soit sauvegardée** (Gingras et Gratton, 2014, p. 38). C'est ce qu'on désigne comme **l'attente de vie privée**. L'employeur doit conduire la fouille avec des **moyens raisonnables et proportionnels**, de façon à porter le moins possible atteinte au droit à la vie privée de l'employé.

Quels sont les facteurs à considérer pour établir, d'une part, l'attente de vie privée d'un employé à l'endroit de l'information emmagasinée dans un ordinateur et, d'autre part, la légitimité de la vérification par l'employeur de l'ordinateur utilisé par son employé?

Nous savons qu'il faut respecter un juste équilibre entre, d'une part, le droit à la vie privée de l'employé et, d'autre part, le droit de direction de l'employeur. Le droit à la vie privée fait référence au droit au respect du caractère privé des informations. C'est donc l'information emmagasinée dans l'ordinateur que protège le droit et non l'ordinateur – le matériel informatique – lui-même.

Qui peut fouiller un appareil informatique?

L'employeur a le droit, **en vertu de ses droits de direction et à certaines conditions** (que nous allons voir plus bas), de mener des enquêtes sur des comportements qu'il croit fautifs lorsque ceux-ci se produisent sur les lieux et pendant les heures de travail. L'employeur n'espionne pas alors un salarié dans les activités de sa vie privée, mais vérifie s'il effectue le travail pour lequel il le paye, travail qui exige l'utilisation d'un ordinateur.

L'employeur et l'employeur seul peut se réserver le droit de surveiller, de vérifier, de bloquer et de désactiver l'utilisation des ressources informatiques et d'autres ressources électroniques. Ainsi, en présence d'un doute raisonnable quant à l'existence d'un comportement déloyal, l'employeur pourra fouiller les communications et les ressources informatiques de l'employé au cours des semaines précédant son départ et obtenir des éléments de preuve pertinents. **L'employeur et l'employeur seul** peut autoriser la fouille et la déléguer à un employé compétent en ces matières.

Sur le plan technique, l'employeur peut facilement avoir accès à la base de courriels de ses employés; peut-il légalement le faire? Même lorsque ces appareils lui appartiennent, il ne peut se prévaloir à sa guise de la prérogative de fouiller les appareils électroniques qu'utilisent ses employés. Il ne doit le faire que lorsqu'il entretient des **doutes et a des motifs raisonnables de croire** que l'employé utilise l'outil informatique **à des fins autres que professionnelles ou de manière abusive** (Lefebvre, 2008, p. 67). La **relation de subordination** propre à la relation d'emploi ne permet pas de déduire un consentement du salarié à toute atteinte à sa vie privée.

QUAND L'EMPLOYEUR EST-IL EN DROIT DE FOUILLER UN APPAREIL INFORMATIQUE?

L'employeur a intérêt à s'assurer que l'information obtenue à la suite de sa vérification sera admissible en preuve, pour éviter des coûts inutiles. Pour que sa vérification soit admissible, elle ne doit pas, selon la Charte canadienne des droits et libertés, **déconsidérer l'administration de la justice**, ni ouvrir la porte à une **poursuite de l'employé pour atteinte à sa vie privée** (Gingras et Gratton, 2014, p. 51-52) :

24. (1) Toute personne, victime de violation ou de négation des droits ou libertés qui lui sont garantis par la présente charte, peut s'adresser à un tribunal compétent pour obtenir

la réparation que le tribunal estime convenable et juste eu égard aux circonstances.

(2) Lorsque, dans une instance visée au paragraphe (1), le tribunal a conclu que des éléments de preuve ont été obtenus dans des conditions qui portent atteinte aux droits ou libertés garantis par la présente charte, ces éléments de preuve sont écartés s'il est établi, eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice. (Charte canadienne des droits et libertés)

L'employeur doit-il s'abstenir de toute intrusion dans les ordinateurs de ses employés?

On peut déduire de la consultation de la jurisprudence deux conditions posées par les tribunaux pour établir le droit légitime de l'employeur d'effectuer une vérification :

- L'employé pouvait-il entretenir une **attente de vie privée** à l'égard de l'information vérifiée par l'employeur?
- L'employeur avait-il le droit légitime de vérifier l'information en cause, de fouiller les appareils? Pour répondre à cette question, le tribunal doit vérifier deux choses : l'employeur avait-il des **motifs rationnels, fondés et sérieux** de vérifier cette information, de douter de la loyauté de l'employé? Est-ce qu'il a utilisé des **moyens raisonnables et proportionnels**, de façon à porter le moins possible atteinte au droit à la vie privée de l'employé?

Le **consentement de l'employé** à la fouille est classé sous la rubrique de la première ou de la deuxième condition, selon les juristes; j'ai choisi de le traiter à part, car il relève à la fois des deux conditions posées par les tribunaux pour établir le droit légitime de l'employeur d'effectuer une vérification :

- le consentement à une intrusion dans sa vie privée réduit l'**attente de vie privée** à l'égard de l'information vérifiée par l'employeur,
- et **confère à l'employeur le droit légitime** de vérifier l'information en cause, de fouiller les appareils.

Si l'employeur ne satisfait pas à ces conditions, l'information obtenue risque de ne pas être jugée admissible en preuve par le tribunal et, d'autre part, l'employé pourra exercer un recours contre la vérification pour atteinte à sa vie privée (Gingras et Gratton, 2014, p. 67).

L'employeur n'est pas tenu d'informer un employé dans le cas d'une fouille en particulier. Cependant, idéalement, l'employeur aura avisé tous ses employés qu'il peut procéder à la fouille des appareils électroniques, comment, etc., par le truchement d'une politique. De cette manière, il réduit les attentes en matière de vie privée, avise tout son effectif des dispositions de la loi et évite des conflits et des poursuites inutiles.

Notez que cette revue **ne constitue en aucun cas un guide pouvant prédire la décision du tribunal**, étant donné que toute décision est rendue par rapport à l'ensemble du contexte propre à chaque cas.

La fouille autorisée ou le consentement

Nous avons vu que, selon la Loi sur la protection des renseignements personnels dans le secteur privé (LRQ, c. P-39.1), l'employeur ne peut pas librement recueillir ni utiliser des renseignements concernant ses employés. Les personnes visées doivent donner leur consentement à la collecte et à l'utilisation de renseignements personnels les concernant, et le consentement doit être explicite. Le **droit de fouille** s'obtient différemment : le **consentement peut être explicite ou implicite**, mais les conditions suivantes sont importantes.

Le consentement explicite

Le consentement est explicite si, par exemple, l'employé a signé un formulaire autorisant son employeur à effectuer une telle vérification. Cependant, **même dans ce cas, l'employeur doit démontrer qu'il a des motifs sérieux** justifiant la vérification (illustré, par exemple, dans la décision *Syndicat des professionnelles et professionnels des affaires sociales du Québec (CSN) et Institut de réadaptation en déficience physique de Québec* (MM. Alain Dubois et Louis Gauthier) [2004] (TA)).

On peut renoncer à son droit à la vie privée et autoriser la fouille, par exemple de son sac ou d'autres effets personnels, mais il faut donner son **consentement de façon libre et éclairée** (illustré, par exemple, dans la décision *Godbout c. Ville de Longueuil* [1997] (CSC), soit en toute connaissance de cause et sans pression indue. Certaines décisions ont soulevé la question du **consentement forcé** d'un employé. Par exemple, la signature à l'embauche d'un document autorisant son employeur à vérifier le contenu de son ordinateur peut ne pas suffire. Ce document sera toutefois pertinent pour démontrer que l'employé avait connaissance des politiques de l'employeur selon lesquelles une vérification était possible. Les tribunaux vont tenir compte du contexte, notamment des conséquences du refus de l'employé à consentir à la vérification. Ainsi, si l'employé est menacé de congédiement ou d'une autre mesure disciplinaire en cas de refus, il sera plus difficile de démontrer un consentement libre et éclairé. Si ces conditions sont remplies, la fouille est valide en droit (Pedneault, Bernier et Granosik, 2015, p. 21-35).

Le consentement libre, volontaire et éclairé est celui qui n'est pas dicté par la crainte, entre autres celle des conséquences d'un refus (menace de renvoi, de suspension ou de rétrogradation), pas non plus inspiré par un tiers, entre autres la personne qui en fait la demande, par la fraude, la mauvaise information, l'abus. Il s'agit aussi du consentement fourni par une personne qui comprend la demande formulée et ses conséquences. Par conséquent, la crainte peut entraîner le vice du consentement donné en matière de tests de dépistage (Pedneault, Bernier et Granosik, 2015, p. 17-5) et, selon les cas, son annulation.

Le consentement implicite

Le consentement est implicite si, par exemple, l'employé remet son ordinateur à l'employeur tout en sachant qu'il sera vérifié (illustré, par exemple, dans l'arrêt *R. c. Cole* [2012] (CSC) ou s'il abandonne son ordinateur personnel sans avoir pris soin de détruire ses renseignements personnels ou ses informations privées :

Il aurait été beaucoup plus facile pour Senécal de « nettoyer » son ordinateur avant de quitter Stock, de changer son adresse courriel en y retranchant le mot ou les lettres « stock » et de changer son mot de passe. Ainsi, ses communications privées auraient été beaucoup mieux protégées. Il aurait aussi été plus prudent de récupérer son ancien ordinateur ainsi que le disque dur qui s'y trouve. Par analogie, un ordinateur peut être considéré comme un classeur électronique fermé à clé par une clé électronique. Ce « classeur » laissé sur place et que l'on refuse de récupérer peut contenir toutes sortes d'informations qui, si elles sont ainsi laissées sur place, peuvent devenir accessibles si elles ne sont pas bien protégées. (décision 9116-8609 *Québec inc. c. Senécal* [2010] (CS), parag. 42)



Rappel : l'arrêt *R. c. Cole* [2012] (CSC) est fourni dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques », si vous voulez la lire pour satisfaire votre curiosité seulement.

Le consentement implicite peut aussi se déduire lorsque l'employé diffuse des informations dans un service en ligne, tel Facebook, car il accepte, d'une certaine façon, que ses propos deviennent publics et puissent être consultés, donc potentiellement admis en preuve devant les tribunaux (illustré, par exemple, dans la décision *Lessard c. Bissonnette* [2013] (CQ). De même, lorsqu'une employée remet son mot de passe à un collègue pour accéder au contenu de son compte Facebook, il y a consentement implicite.

Si l'employeur a implanté une politique qui restreint l'usage personnel des ordinateurs, qui précise que l'employeur se réserve le droit de vérifier leur contenu, annonce la possibilité de vérifier les ordinateurs utilisés par ses employés dans certaines situations, avise que de telles vérifications peuvent avoir lieu, et que **cette politique est en vigueur et bien connue des employés autant que de la direction**, les tribunaux tendent à considérer la vérification comme légitime. J'expose plus bas les conditions que doit remplir une politique à ce sujet.

Inversement, s'il n'y a pas de politique connue par l'employé ni d'interdiction, l'employé qui utilise Internet **à des fins personnelles** pourra argumenter que son comportement est toléré et peut faire échec au congédiement ou à la sanction qu'on lui impose. Cependant, si l'employeur a au moins avisé les employés de la possibilité d'une vérification des appareils, sans nécessairement qu'une politique soit en vigueur, le tribunal peut considérer que la vérification est légitime (Gingras et Gratton, 2014, p. 79-87).

Lorsque la **convention collective** le prévoit, ou encore le contrat de travail (dans le

formulaire d'embauche, par exemple), un règlement ou une politique, cela équivaut à un consentement et l'employeur peut fouiller; les salariés sont alors présumés connaître l'existence de la procédure de fouille (Pedneault, Bernier et Granosik, 2015, p. 21-35). Bien sûr, l'employé qui refuse de donner son consentement dans le formulaire de demande d'emploi et qui n'est pas rappelé pour le processus de sélection aura bien du mal, en pratique, à faire valoir ses droits.

Quant à la surveillance par **caméra**, aussi régie par les dispositions juridiques régissant les fouilles, lorsque toutes les parties concernées consentent aux fouilles ou à la surveillance électronique, que c'est là une condition de travail bien établie et connue des employés et qu'elle est mise en place pour des motifs sérieux (épidémie de vols, par exemple, ou nature de l'entreprise), l'employeur pourrait, en principe, la pratiquer (Pedneault, Bernier et Granosik, 2015, p. 21-35).

En l'absence d'un consentement généralisé de la part des travailleurs

En revanche, si l'employé n'a pas donné son consentement, cela peut compromettre la légitimité de la vérification (voir à ce sujet la décision *Journeaux c. Perreault* [2011] (CS)). On peut déduire **l'absence de consentement implicite**, par exemple si l'employé prend soin de mettre un cadenas sur l'ordinateur qu'il utilise dans ses fonctions pendant son absence. Il démontre ainsi son refus à voir son employeur accéder au contenu.



Lisez à ce sujet la décision *Journeaux c. Perreault* [2011] (CS), fournie dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques ». Non seulement elle illustre ce que vous venez de lire, mais elle a inspiré l'étude de cas qui fait l'objet de votre travail noté.

Toutefois, dans ce cas, le tribunal a interprété le refus de l'employé comme justifiant un doute chez l'employeur et, de ce fait, la vérification... (illustré, par exemple, dans la décision *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles et Commission scolaire de la Seigneurie-des-Mille-Îles* [2008] (TA).

Lorsque l'employeur n'a **pas implanté de politique d'usage personnel des ordinateurs concernant les fouilles** ni de règlement et qu'il n'y a pas de disposition de convention collective à ce sujet, le salarié peut refuser une telle demande de l'employeur.

Cependant, **dans certaines circonstances, la fouille est permise à l'employeur en l'absence de consentement** et même si l'employeur n'a pas de politique prévoyant la fouille de façon explicite.

D'abord, lorsque la fouille fait implicitement partie des pratiques dans un milieu donné, de façon périodique et dans certaines circonstances, par exemple, on invoque la notion

juridique de **pratique établie** pour légitimer le recours par l'employeur à la fouille (Pedneault, Bernier et Granosik, 2015, p. 21-67). Il faut, cependant, pour reconnaître une pratique établie, que les fouilles aient été pratiquées fréquemment, avec constance et universellement par le passé dans l'entreprise et non pas de façon exceptionnelle, il y a longtemps ou encore juste une fois (Pedneault, Bernier et Granosik, 2015, p. 21-68). Si l'employeur ne se fonde que sur la pratique passée, la pratique des sanctions disciplinaires devra aussi respecter la pratique passée. S'il n'a jamais sévi, il ne peut commencer à le faire sans l'avoir d'abord annoncé, par voie de règlement ou de politique (Pedneault, Bernier et Granosik, 2015, p. 21-69).

Aussi, dans les cas de flagrant délit, l'employeur peut procéder. Il peut fouiller un seul employé, *ad hoc*, s'il a des motifs raisonnables de croire que la personne fouillée a commis un délit (Pedneault, Bernier et Granosik, 2015, p. 21-72). La jurisprudence n'est cependant pas constante, et on peut trouver des contre-exemples. Dans le même ordre d'idées, les épidémies de vol, la nature particulière de l'entreprise (bijouterie, musée, mine d'or) ou encore les soupçons motivés (qu'on doit démontrer) pesant sur un salarié sont des motifs sérieux pouvant justifier l'employeur de fouiller (Pedneault, Bernier et Granosik, 2015, p. 21-70).

J'aborderai plus bas le scénario du refus de la fouille par l'employé.

On peut résumer ainsi les **conditions** auxquelles l'employeur peut fouiller en l'absence de consentement :

- faire la preuve du fondement des soupçons individuels ou de l'épidémie de vols;
- dans ce deuxième cas, établir un lien entre l'épidémie et les travailleurs fouillés (en d'autres termes, éviter « d'aller à la pêche »);
- démontrer que d'autres stratégies de prévention se sont avérées infructueuses;
- respecter la dignité des personnes;
- être raisonnable compte tenu de l'objectif et ne pas dépasser ce qui est nécessaire pour préserver ses intérêts légitimes (Pedneault, Bernier et Granosik, 2015, p. 21-135);
- ne pas être discriminatoire et ne pas cibler un groupe particulier si les soupçons ne sont pas individuels (Pedneault, Bernier et Granosik, 2015, p. 21-69 à 21-71).

L'employé pouvait-il entretenir une attente de vie privée à l'égard de l'information vérifiée par l'employeur?

La propriété de l'ordinateur

Au Québec, un employeur qui fournit un ordinateur à son employé et lui **permet d'utiliser cet appareil à des fins personnelles** ne peut pas, de plein droit et sans motif, prendre connaissance de l'information emmagasinée dans cet ordinateur (illustré, par exemple, dans

la décision *Université Laval et Association du personnel administratif professionnel de l'Université Laval (APAPUL)* [2011] (TA). Dès qu'un ordinateur est utilisé à des fins personnelles, il faut considérer l'appareil comme partie de la vie privée. Aussi minime soit cet usage, on peut y trouver des renseignements qui sont significatifs, intimes et liés à l'ensemble des renseignements biographiques qu'on doit protéger à ce titre.

En revanche, dès qu'un employé utilise son ordinateur personnel aux fins professionnelles, il peut s'attendre à ce que l'information qu'il y emmagasine soit protégée comme partie de sa vie privée; cependant, si un employé laisse volontairement derrière lui son ordinateur personnel au moment de la cessation de son emploi, et ne désire pas le récupérer, le tribunal peut considérer qu'il renonce à son attente de vie privée à l'endroit de l'information emmagasinée dans cet ordinateur (Gingras et Gratton, 2014, p. 52-54, citant la décision *9116-8609 Québec inc. c. Sénécal* [2010] (CS)).

Les tribunaux sont plus sévères quant à la légitimité de la fouille d'un ordinateur qui appartient à l'employé et qui a lieu au domicile de celui-ci (Gingras et Gratton, 2014, p. 87, citant l'arrêt *R. c. Cole* [2012] (CSC)).

La nature de l'information recherchée

Plus l'objet de la fouille se trouve près de l'ensemble de **renseignements d'ordre personnel** (que le tribunal désignera aussi comme « biographiques »), plus le tribunal considère que l'employé peut nourrir une attente raisonnable en matière de respect de la vie privée. La liste des recherches effectuées sur Internet, par exemple, est de nature biographique ou intime (Gratton, 2013, p. 323).

Les communications par courriel sont aussi de ce type, ainsi qu'une information médicale relative à la famille de l'individu, à sa vie amoureuse ou sexuelle, à ses opinions politiques, philosophiques ou religieuses, à ses communications privées, ou encore à ses finances, et une information qui pourra créer humiliation ou embarras pour l'individu, entre autres parce qu'elle n'était pas déjà connue au moment de sa divulgation. Les échanges entre syndiqués et représentants syndicaux relèvent aussi de cette catégorie (Gingras et Gratton, 2014, p. 54-56).

L'endroit où l'information est emmagasinée

Selon quelques décisions récentes, le fait que les courriels se trouvent dans la boîte de courriels personnels de l'employé ne restreint pas le droit de l'employeur d'y accéder et d'utiliser ces courriels comme preuve.

En ce qui a trait aux services en ligne et aux réseaux sociaux, il n'y a pas d'attente de vie privée à l'endroit d'une information diffusée par l'entremise de ces services lorsqu'elle est accessible au public. Lorsque l'information est **accessible à un nombre restreint de**

personnes, selon les paramètres du compte et le nombre de personnes ayant accès à l'information, il y a une attente proportionnelle de vie privée. Si l'utilisateur a choisi les paramètres privés et qu'il a un nombre limité d'amis lui permettant de garder le contrôle sur sa vie privée, cela peut nourrir son attente de protection de la vie privée (Gingras et Gratton, 2014, p. 56-59).

Les mesures technologiques de protection

Si l'employé n'a pas pris de mesures technologiques de protection, tel un mot de passe ou le chiffrement, restreignant l'accès à une information emmagasinée dans un ordinateur ou accessible par son entremise, cela réduit forcément son attente de vie privée.

En revanche, lorsque le document est gardé dans un lieu personnel difficilement accessible ou que son propriétaire, par son comportement, a **manifesté qu'il voulait en faire un document confidentiel**, cela favorise la protection de la vie privée. Notamment, le fait de changer souvent son mot de passe et de le choisir de manière à ce qu'il soit difficile à deviner nourrit l'attente de vie privée.

Inversement, lorsque tel n'est pas le cas, les tribunaux peuvent considérer que l'employé n'a pas d'attente en matière de protection de sa vie privée. Les tribunaux ne respectent cette protection qu'à l'égard d'informations personnelles et non professionnelles (Gingras et Gratton, 2014, p. 59-64).

Le fait que l'information a été effacée ou non

Bien qu'une information puisse avoir été effacée d'un ordinateur, c'est-à-dire supprimée de la corbeille, il est fort possible qu'elle soit toujours accessible pour un utilisateur aguerri. Certaines décisions des tribunaux tendent à considérer que le fait pour un individu de supprimer le contenu d'un ordinateur, dans un contexte criminel, indique l'intention de dissimuler, et donc de maintenir une attente de vie privée, plutôt que d'abandonner et de renoncer ainsi à une attente de vie privée (illustré, par exemple, dans la décision *R. c. McNeice* [2013] (CA de CB)).

C'est une tendance qui peut surprendre.

En revanche, dans d'autres décisions prises dans un contexte d'emploi, le tribunal a considéré qu'un employé ayant effacé son historique de navigation sur Internet démontrait sa mauvaise foi, sa conscience d'être en faute, et justifiait les sanctions prises contre lui par son employeur (illustré, par exemple, dans les décisions *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles et Commission scolaire de la Seigneurie-des-Mille-Îles* [2008] (TA); *Syndicat des spécialistes et professionnels d'Hydro-Québec et Hydro-Québec* [2007] (TA)).

Il est donc difficile de prévoir le comportement des tribunaux en cette matière.

L'EMPLOYEUR A-T-IL LE DROIT LÉGITIME DE FOUILLER?

Pour répondre à cette question, le tribunal doit établir que l'employeur remplit deux conditions :

- il avait des **motifs rationnels, fondés et sérieux** de vérifier cette information, motifs qui sont liés au travail, au respect du contrat d'emploi, des normes de l'employeur, des politiques de l'organisation, bref qui se situe dans le champ d'autorité de l'employeur et de la protection de ses **intérêts légitimes**, non pas liés à la vie privée de l'employé ou à des intérêts particuliers;
- et il a utilisé des **moyens raisonnables et proportionnels**, de façon à porter le moins possible atteinte au droit à la vie privée de l'employé.

Le motif justifiant la vérification

Lorsque l'employeur – ou son représentant - n'a aucune indication objective, fondée sur des faits, selon laquelle un employé est engagé dans une fraude, un vol de temps de travail ou un autre délit, il ne peut demander la vérification de l'ordinateur d'un employé sans en compromettre la légitimité. De simples soupçons ou des impressions ne suffisent pas à justifier une vérification. Les tribunaux sont réticents à admettre comme preuve les résultats de ce qu'ils appellent une « partie de pêche » de l'employeur, motivée par quelques soupçons non documentés ou non fondés.

La jurisprudence permet de dégager quatre scénarios qui peuvent légitimer une telle vérification, et qui peuvent se combiner :

- **La découverte fortuite d'éléments factuels fournissant un doute raisonnable à l'employeur, notamment en matière de concurrence déloyale** : tomber par hasard sur un courriel d'un employé démontrant son manque de loyauté, découvrir un document témoignant d'un projet concurrent dans le même secteur d'activité, découvrir du matériel de pornographie juvénile de façon fortuite, intercepter un courriel trop volumineux. Par exemple, trouver un document laissé dans le télécopieur, qui amène à douter de sa loyauté.
- **La diminution soudaine ou prolongée de la productivité de l'employé, une augmentation injustifiée du nombre d'heures supplémentaires réclamées, souvent associées au vol de temps** : l'employeur doit s'assurer que la baisse de rendement est importante et déraisonnable. Il doit, par exemple, commencer par utiliser des moyens non intrusifs, telle une revue des fichiers journaux pour analyser les sites Internet visités et le temps passé par l'employé à naviguer sur le web durant ses heures de travail, sans

faire une revue complète du contenu consulté ou des activités de l'employé.

- **Une insubordination importante de l'employé** : par exemple, dans un cas de congédiement, une employée peut faire preuve d'insubordination à l'égard de son supérieur et préparer, pendant ses heures de travail, une lettre afin de démontrer son mécontentement. Le tribunal a considéré que le directeur est justifié d'accéder au contenu de l'ordinateur de l'employée à son insu et de prendre connaissance du projet de lettre (illustré, par exemple, dans les décisions *Ghattas c. École nationale de théâtre du Canada* [2006] (CS) et *Syndicat des professionnelles et professionnels des affaires sociales du Québec (CSN) et Institut de réadaptation en déficience physique de Québec (MM. Alain Dubois et Louis Gauthier)* [2004] (TA)). Mais ce genre de scénario est difficile à justifier.
- **Les plaintes ou les constats d'utilisation abusive par d'autres personnes rapportant un usage inapproprié de l'employé** : les tribunaux considèrent que l'employeur est justifié de vérifier un appareil lorsque l'employé qui envoie des courriels inappropriés a déjà agi ainsi par le passé et si, en outre, le courriel peut porter atteinte à la réputation ou à l'image de l'employeur, ou engager sa responsabilité. L'employeur qui reçoit des plaintes selon lesquelles un employé fait un usage inapproprié de son ordinateur, par exemple en accédant à du contenu illégal ou à du matériel pornographique, en étant surpris à jouer à des jeux vidéo pendant ses heures de travail, en envoyant des courriels offensants, en exploitant un commerce de films piratés avec l'appareil fourni par l'employeur, ou encore en consultant le dossier fiscal de son supérieur, peut vérifier son appareil après s'être assuré que :
 - l'usage est sérieusement délinquant,
 - le dénonciateur est crédible (Gingras et Gratton, 2014, p. 69-76).

La nature de l'utilisation de l'ordinateur par l'employé

Pour établir si l'employeur a le droit légitime de vérifier un appareil, les tribunaux considèrent aussi la nature de l'utilisation par l'employé :

- **L'usage est abusif ou a fait l'objet de plusieurs avertissements** : les récidives multiples et les infractions aux règles d'utilisation des ordinateurs fixées par l'employeur sont des facteurs aggravants qui justifient la vérification d'un appareil par l'employeur. L'employeur doit cependant documenter les récidives et les avertissements communiqués aux employés.
- **L'usage inapproprié est grave** : si, par exemple, l'employé est soupçonné d'un acte criminel, tel le vol, la fraude ou le visionnement de matériel pornographique, la gravité peut suffire à justifier la vérification de l'ordinateur.
- **L'employé exploite une entreprise personnelle** avec l'ordinateur de l'employeur : par exemple, un employé participe à la mise sur pied d'un centre de la petite enfance (CPE) et réclame subitement plusieurs heures supplémentaires, on trouve dans le photocopieur

des documents relatifs à un organisme inconnu, un employé transmet des informations confidentielles à un concurrent par courriel à partir de son poste de travail. Dans ces situations, les tribunaux ont considéré que l'employeur a le droit légitime d'examiner les courriels ou l'ordinateur d'un l'employé (voir à ce sujet *Pneus Touchette Distribution inc. c. Pneus Chartrand inc.* [2012] (CS)) (Gingras et Gratton, 2014, p. 77-78).

Le niveau d'autorité de la personne qui demande la vérification

La personne qui demande la vérification doit avoir **l'autorité nécessaire sur un employé** donné pour exiger une telle vérification.

Un technicien en informatique qui, **de son propre chef**, vérifie les informations emmagasinées dans les ordinateurs de certains employés peut difficilement justifier la légitimité de sa vérification; cela, de l'avis des tribunaux, déconsidère l'administration de la justice. De même, une représentante de l'employeur ne peut rechercher, **de son propre chef**, des informations sur un employé dans le but d'améliorer un dossier en vue de l'audience devant le tribunal, car elle ne détient pas d'intérêt juridique dans l'affaire : c'est plutôt l'employeur qui en a un. Ce dernier doit l'exiger lui-même. Il est responsable des actes accomplis par ses employés et, à cet égard, a intérêt à les informer par une politique bien diffusée. Il peut être amené à assumer les conséquences de ces actes mais peut, en retour, poursuivre les employés qui les ont accomplis en vertu du Code civil du Québec :

1463. Le commettant est tenu de réparer le préjudice causé par la faute de ses préposés dans l'exécution de leurs fonctions; il conserve, néanmoins, ses recours contre eux.

En revanche, si le président de l'entreprise lui demande la vérification des informations sur l'employé et une copie de celles-ci, même si la vérification est jugée illégitime par le tribunal, ce dernier ne tiendra pas le technicien responsable, car il est subordonné à son employeur.



Lisez à ce sujet la décision *Journeaux c. Perreault* [2011] (CS), fournie dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques ».

Les moyens et procédés utilisés pour accéder à l'information

Ces moyens doivent remplir deux conditions.

L'employeur doit utiliser des **moyens licites**; les tribunaux auront du mal à légitimer l'usage d'un moyen illicite. Il doit chercher à **porter atteinte le moins possible** aux droits et aux libertés individuelles de l'employé. Lorsque l'information est emmagasinée dans un ordinateur personnel ou dans un service en ligne, l'employeur sera avisé de recourir aux tribunaux afin d'obtenir une ordonnance lui permettant d'obtenir cette information. Par exemple, si l'employeur crée un compte Facebook fictif pour devenir « ami Facebook » avec

un employé, compose un profil fictif pour attirer son attention et accéder à son compte, il utilise selon le tribunal un moyen frauduleux, détourné, un subterfuge afin de devenir « l'ami » du travailleur dans le réseau social. D'aucune façon le salarié n'y a consenti, ne sachant pas qui était l'ami qui le sollicitait. L'employeur utilise des informations personnelles et confidentielles à son sujet (études à la même université, préférences musicales, de lecture, de cinéma, etc.) dans le seul but de créer un profil attirant.

Ce moyen n'est pas de nature à porter atteinte « le moins possible » aux droits et libertés individuelles du travailleur, ne constitue pas une atteinte minime. Au contraire, il ne respecte pas les libertés garanties par la charte québécoise. Une personne conserve une attente raisonnable à la protection du droit à sa vie privée à l'égard d'une information non accessible par un moyen licite (illustré, par exemple, dans la décision *Campeau et Services alimentaires Delta Dailyfood Canada inc.* [2012] (CLP)).

Une fois l'accès obtenu, l'employeur doit **fouiller et rechercher de façon raisonnable** : l'employeur devrait consulter **les seules informations liées au motif** pour lequel il a effectué la vérification. L'employeur qui vérifie si l'un de ses employés a communiqué des informations confidentielles à un concurrent ne doit lire que l'objet des courriels ou se limiter à ne rechercher dans le corps des courriels que des termes liés directement aux motifs de sa vérification.

Cependant, lorsque la preuve recherchée peut être découverte à peu près n'importe où et de n'importe quelle manière, le tribunal reconnaît la nécessité d'une fouille intensive (illustré, par exemple, dans l'arrêt *R. c. Vu* [2013] (CSC), parag. 59). Par conséquent, l'employeur doit documenter les actions et les gestes pour permettre au tribunal de juger du caractère raisonnable de la recherche (Gingras et Gratton, 2014, p. 87-93).

L'urgence d'agir pour l'employeur

L'employeur peut avoir besoin d'agir rapidement afin d'éviter que l'employé efface une information qui démontre un geste fautif, notamment lorsqu'il y a un risque réel de suppression de l'information. L'employeur peut avoir intérêt à prendre lui-même une copie de sauvegarde de l'information. Lorsqu'il ne peut accéder à l'information sans porter atteinte à la vie privée de son employé, notamment dans les cas où cette information est emmagasinée dans un service en ligne tel qu'un profil privé Facebook, il doit obtenir une ordonnance pour que son employé, ou un service en ligne, conserve certaines informations.

L'employeur doit établir « que sans l'émission d'une telle ordonnance, la preuve risque de disparaître » (*Béton St-Hubert inc. c. Entreprises Kijiji Canada inc.* [2009] (CS)). Une telle preuve de risque de suppression est difficile à faire (Gingras et Gratton, 2014, p. 93-95).

QUEL EST LE RAISONNEMENT DU TRIBUNAL EN CAS DE PLAINTE?

La démarche axée sur la proportionnalité

Dans le traitement des **dossiers touchant les droits fondamentaux**, en général, le tribunal devra établir l'importance relative du droit à la vie privée de l'employé, d'une part, et de la poursuite des intérêts légitimes de l'employeur, d'autre part. Comment établir la hiérarchie de ces deux éléments? Pour établir s'il peut admettre en preuve les résultats de la fouille d'un ordinateur personnel, le tribunal doit entreprendre une « **démarche axée sur la proportionnalité** » (Monet, 2013, p. 55) et comparer les gains que procure la fouille pour les intérêts respectifs de l'employeur et de l'employé, d'une part, et les pertes de droits qui en découlent pour les deux parties, d'autre part. Par exemple, plus l'une des parties est lésée de façon importante dans son droit fondamental à la vie privée, plus grands doivent être les gains permis par la fouille (Monet, 2013, p. 56).

Le tribunal se livre à cet exercice parce qu'il doit rejeter tout élément de preuve obtenu dans des conditions qui portent atteinte aux droits et libertés fondamentaux, parce que leur utilisation est susceptible de déconsidérer l'administration de la justice selon le Code civil du Québec (Monet, 2013, p. 57) :

2858. Le tribunal doit, même d'office, rejeter tout élément de preuve obtenu dans des conditions qui portent atteinte aux droits et libertés fondamentaux et dont l'utilisation est susceptible de déconsidérer l'administration de la justice.

Il n'est pas tenu compte de ce dernier critère lorsqu'il s'agit d'une violation du droit au respect du secret professionnel.

Dans le cas de la concurrence déloyale, en particulier, le tribunal étudie l'importance relative du droit de l'employeur d'empêcher une concurrence déloyale de la part d'un ex-employé et du droit des employés à la protection de la vie privée. **Dans la démarche axée sur la proportionnalité**, les intérêts économiques de l'employeur sont souvent essentiels à la santé ou à la survie de son entreprise, d'une part; comme l'information recherchée n'est pas de nature personnelle, mais professionnelle, toute atteinte en matière de protection de la vie privée est sérieusement minée, d'autre part. Le tribunal donnera donc souvent raison à l'employeur dans son droit d'utiliser comme preuve les démarches déloyales de son employé, et ce, d'autant plus que la transmission des informations a eu lieu pendant les heures de travail, facteur aggravant qui justifie la fouille (Monet, 2013, p. 69).

Un expert soutient à ce sujet que :

Si un employé utilise un ordinateur, un portable, un iPhone ou un cellulaire fourni par son employeur pour planifier une concurrence, cet employé utilise les ressources de l'employeur à des fins détournées et trahit sa mission. Vues sous cet angle, la reprise de possession de l'outil de travail et son inspection pour retracer les pas de l'employé alors

qu'il était à l'emploi nous paraissent essentielles pour s'assurer que justice soit rendue. (Monet, 2013, p. 63)

Ces informations ne portent pas sur des aspects intimes et liés organiquement au profil biographique, comme dans l'affaire *Cole*, citée plus haut (Monet, 2013, p. 58).

Trois exemples d'application de la démarche axée sur la proportionnalité

L'arrêt Cole : l'importance de l'information à caractère intime et personnel

Dans l'arrêt *Cole c. Rainbow District School Board* [2012] (CSC) de la Cour suprême du Canada, l'employeur reprend possession d'un portable qu'il a fourni à son employé pour l'exercice de ses fonctions. Il trouve, saisit et reproduit des photographies de nature sexuelle et pornographique, des dossiers que l'employé a emmagasinés dans le disque dur et des fichiers temporaires créés pendant ses recherches dans Internet (Monet, 2013, p. 42). L'école secondaire a d'abord effectué saisie et fouille de son propre chef, puis remis l'appareil au service de police qui a repris à son tour la démarche.

L'usage de cet ordinateur portable est réglementé par une politique d'utilisation acceptable et des procédures écrites, officielles et explicites. L'ordinateur demeure la propriété de l'école, mais l'employé peut utiliser un mot de passe pour limiter l'accès à son contenu. L'employeur permet l'usage occasionnel de l'ordinateur à des fins personnelles. Ainsi, l'employé a le privilège d'apporter et d'utiliser l'ordinateur portable à domicile après les heures de travail ou pendant les périodes de vacances (Monet, 2013, p. 43).

La politique stipule que les usagers doivent tenir pour acquis que les dossiers gardés sur les serveurs de réseau ou les disques durs des ordinateurs personnels peuvent être examinés, qu'ils ne doivent comporter aucun contenu inopportun, y compris du matériel sexuel explicite. Le manuel ne prévoit pas de façon expresse le droit général de l'employeur de fouiller les appareils, mais avise que l'équipe administrative peut ouvrir le courriel s'il s'avère nécessaire de le faire pour la santé du réseau informatique ou si elle soupçonne un usage inopportun. Enfin, la direction rappelle périodiquement aux enseignants qu'ils ne peuvent s'attendre à ce que les fichiers emmagasinés sur leurs ordinateurs portables soient confidentiels (Monet, 2013, p. 44).

Cependant, malgré des textes suffisamment clairs selon lesquels le contenu des ordinateurs portables ne doit pas être considéré comme relevant de la vie privée des employés, la Cour suprême a quand même jugé que les employés conservent une **attente raisonnable en matière de vie privée** dès qu'il y a **possibilité d'utiliser un appareil à des fins personnelles**. Les intérêts légitimes de l'employeur peuvent **réduire cette attente, mais pas l'éliminer**. Le contenu d'un ordinateur personnel expose les préférences, les intérêts, les pensées, les activités, les idées et les recherches de renseignements de l'utilisateur et, en

cela, mérite une certaine protection à titre de révélateur de la vie privée (Monet, 2013, p. 45-46).

Les ordinateurs qui sont utilisés d'une manière raisonnable à des fins personnelles – qu'ils se trouvent au travail ou à la maison – contiennent des renseignements qui sont **significatifs, intimes et que la Cour associe à l'ensemble des renseignements biographiques** de l'utilisateur (parag. 2). Au Canada, la Constitution accorde à chaque personne le droit de s'attendre à ce que l'État respecte sa vie privée à l'égard des renseignements personnels de ce genre (Monet, 2013, p. 46).

Par ailleurs, l'arrêt *Cole* nous apprend que la Cour suprême considère la nature des informations saisies au moment de se prononcer sur le droit au respect de la vie privée protégé par la Constitution (parag. 58). Par exemple, la nature sexuelle et pornographique des images et des fichiers augmente la protection en matière de respect de la vie privée parce que ces renseignements sont **significatifs, intimes et associés à l'ensemble des renseignements biographiques**; bref, ils font partie des caractéristiques individuelles subjectives propres à l'individu (Monet, 2013, p. 47). Il n'existe pas de droit pour les employeurs de reprendre les portables fournis à leurs employés et de les fouiller à loisir (Monet, 2013, p. 48).

Cependant, dans l'affaire *Cole*, des dispositions législatives de la Loi sur l'éducation (LRO 1990, c. E.2), qui imposent à l'école secondaire l'obligation d'assurer et de maintenir un milieu scolaire sûr, autorisaient l'institution scolaire à fouiller et à saisir des renseignements emmagasinés dans le portable.

Retenons quatre propositions importantes de l'arrêt *Cole* :

- L'employé a une attente raisonnable de protection de sa vie privée à l'égard du contenu de l'ordinateur de travail même si l'ordinateur est la propriété exclusive de son employeur.
- L'employé a une attente raisonnable de protection de sa vie privée à l'égard du contenu de l'ordinateur de travail même s'il y a une politique et des pratiques indiquant le contraire chez son employeur.
- La nature des fichiers, des dossiers et des renseignements examinés et saisis est d'une importance capitale dans l'appréciation des droits de l'employé. Même devant une inconduite grave régie par le droit criminel, commise par un professeur d'une école secondaire, la Cour reconnaît le droit fondamental à la vie privée.
- La règle générale est que l'employeur ne peut *a priori* fouiller et saisir des informations contenues dans un ordinateur portable qu'il fournit à son personnel (Monet, 2013, p. 50).

La décision Pneus Touchette : justifier l'atteinte au droit à la vie privée

Il peut arriver que l'employeur cherche de l'information concernant un soupçon de concurrence déloyale dans le courriel personnel Hotmail de son ex-employé, sans devoir prendre possession de son ordinateur personnel. Par exemple, dans la décision *Pneus Touchette Distribution c. Pneus Chartrand* [2012] (CS), l'employeur demande un rapport d'expertise à la firme spécialisée CompuQuest pour vérifier si son ex-employé avait ou non transmis des informations confidentielles à une tierce partie pendant qu'il était toujours en relation d'emploi. La fouille confirme ses soupçons (Monet, 2013, p. 67).



Lisez à ce sujet les décisions *Pneus Touchette Distribution c. Pneus Chartrand* [2012] (CS) et *Éthier c. Goodyear Canada inc.* [2004] (CRT), fournies dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques ». Non seulement elles illustrent ce que vous venez de lire, mais elles ont inspiré l'étude de cas qui fait l'objet de votre travail noté.

La fouille effectuée dans la boîte de courriel personnelle du défendeur **portait atteinte à son droit à la vie privée**, parce que loin de se limiter à l'ordinateur portable fourni par l'employeur, comme dans l'affaire *Cole*, l'employeur a non seulement réussi à examiner les courriels envoyés par l'employé à même son ordinateur de travail, mais aussi à infiltrer ses courriels personnels et à voir à qui il avait retransmis des renseignements de nature économique concernant son employeur. Avec un tel procédé, l'employeur n'a pas besoin d'aller saisir à la résidence de l'employé son ordinateur personnel. Il s'agit d'un effort délibéré de l'employeur de suivre les activités de son employé jusque dans sa boîte courriel personnelle (Monet, 2013, p. 67).

La Cour supérieure peut-elle admettre en preuve le rapport de la firme CompuQuest, sans déconsidérer l'administration de la justice (art. 2858 CcQ)? Dans ce cas, la Cour supérieure a suivi la **démarche axée sur la proportionnalité** et a jugé la preuve admissible. L'ex-employé a envoyé des courriels à partir de son poste de travail à sa propre adresse Hotmail pendant ses heures de travail et, par conséquent, ne pouvait raisonnablement s'attendre à ce que ses communications demeurent strictement privées. Selon le tribunal, on peut postuler que l'employé qui, à partir de son ordinateur de travail, se transmet à lui-même des renseignements et documents relatifs à son employeur par courriel, s'expose à une fouille élargie. Il ne faut toutefois pas automatiquement conclure que tout employé qui le fait est en faute, car il pourrait, par exemple, travailler à domicile (Monet, 2013, p. 68-69).

Le moyen d'accès utilisé par l'employeur était **illicite**. Le tribunal admet quand même en preuve les courriels ainsi obtenus et estime que la preuve **ne déconsidère pas l'administration de la justice** au sens de l'article 2858 CcQ, en raison des doutes qu'a l'employeur, tout comme dans cette autre décision :

Il ne s'agit pas d'un cas d'interception de message, d'une conversation par écoute électronique ou encore de la fouille d'un ordinateur après avoir subtilisé un mot de passe. Il s'agit de l'obtention de courriels qui existent bel et bien avant toute intervention prétendument illégale. (*Commission des normes du travail c. 9043-5819 Québec inc.* [2013] (CQ), parag. 54)

De telles décisions ouvrent, selon certains experts, une porte dangereuse parce qu'un employeur pourra préférer pirater le compte personnel d'un service en ligne d'un employé, à défaut d'obtenir une ordonnance judiciaire.

Images Turbo : le droit à la vie privée est limité pendant la relation d'emploi, mais pas après

Dans une autre affaire (*Images Turbo inc. c. Marquis* [2013] (CS), l'employeur est une entreprise spécialisée dans le lettrage de camions, et l'ex-employée a été représentante de commerce pendant sept ans. Elle est maintenant responsable de 178 clients. L'employeur lui a remis un ordinateur et un BlackBerry® pour l'exercice de ses fonctions. Les clients peuvent la joindre en tout temps, tant à son adresse de courriel de bureau qu'à son adresse de courriel personnelle. Un compétiteur la sollicite et elle accepte son offre. Comme elle est liée par des engagements de non-concurrence pour six mois, elle trouve un emploi temporaire en attendant. Elle remet sa démission, mais son employeur la convainc de rester à l'emploi pendant une autre semaine. Elle remet son ordinateur et son BlackBerry® à son employeur, pour qu'il en fasse le ménage avant de le remettre à un autre employé (Monet, 2013, p. 69-70).



Lisez à ce sujet la décision *Images Turbo inc. c. Marquis* [2013] (CS), fournie dans le site du cours, sous « Trousses », dans la trousse « Fouille des appareils électroniques ».

Au cours de ce nettoyage, on découvre les échanges de courriel entre l'ex-employée et l'entreprise concurrente, ainsi que d'autres courriels périphériques. Après le départ de la représentante, l'employeur garde l'appareil ouvert pour suivre ses communications. L'employeur demande une injonction et réclame des dommages-intérêts contre l'ex-employée et l'entreprise concurrente. De son côté, madame Marquis se plaint d'une atteinte à ses droits fondamentaux et s'oppose à l'admission en preuve des courriels contenus dans sa boîte personnelle et obtenus en inspectant le BlackBerry® à la suite de sa démission (Monet, 2013, p. 70).

La Cour supérieure accepte **d'admettre en preuve** les courriels reçus et transmis par madame Marquis **avant la cessation d'emploi, mais pas ceux reçus et transmis après la cessation d'emploi** (lorsque l'employeur a décidé de garder ouvert le BlackBerry® pour continuer de surveiller les courriels personnels de madame Marquis).

La Cour décide d'admettre en preuve les courriels reçus et transmis par l'ex-employée

avant la cessation d'emploi, parce que l'employée utilisait tant son adresse de courriel personnelle que celle de l'entreprise pour communiquer avec ses clients. L'employée se sert de sa boîte courriel personnelle tant pour ses affaires personnelles que pour celles de l'entreprise. Le BlackBerry® et l'ordinateur sont la propriété de l'entreprise, mais sont à sa disposition en tout temps. L'employée du service informatique de l'employeur n'a eu besoin d'aucun stratagème ni procédure du type essais et erreurs pour découvrir le mot de passe, car il n'y en avait aucun. C'est seulement dans le but de faire le ménage de la boîte vocale et de remettre l'appareil à un autre employé qu'elle découvre l'ensemble des messages contenus dans la boîte courriel (Monet, 2013, p. 70). L'ex-employée n'avait pas éliminé l'accès à sa boîte courriel personnelle par l'ancien BlackBerry® de travail (Monet, 2013, p. 74). La Cour ajoute que c'est plutôt l'exclusion de cette preuve qui déconsidérerait l'administration de la justice, car « le tribunal a comme fonction première d'obtenir la vérité... » (Monet, 2013, p. 71).

La Cour refuse d'admettre en preuve les messages reçus et transmis **après la cessation d'emploi**, sans expliquer la raison. Manifestement, l'employeur a profité de l'ignorance ou de l'inattention de son ex-employé pour épier ses courriels personnels pendant une période prolongée suivant sa cessation d'emploi. Chose certaine, si la Cour considère que l'employeur porte atteinte à la vie privée, elle devra vraisemblablement le condamner pour dommages-intérêts (Monet, 2013, p. 74). Si elle ne le fait pas, on peut donc supposer qu'elle ne juge pas l'atteinte considérable.

Toutefois, la Cour rejette tant la demande de l'employeur quant au fond (l'employée a respecté le délai de six mois d'interdiction de concurrence prévu dans sa clause de non-concurrence) que celle de l'ex-employée (l'employeur n'était pas de mauvaise foi en surveillant les courriels personnels de son ex-employée après la cessation d'emploi, d'autant plus qu'il venait d'apprendre « qu'un employé important qui a quitté son emploi dix jours avant, est en communication continue avec l'un de ses compétiteurs depuis le mois de février... ») (Monet, 2013, p. 72).

L'EMPLOYÉ PEUT-IL REFUSER LA FOUILLE?

Lorsque **l'employeur est justifié par une politique ou par des motifs sérieux** (en l'absence de politique), l'employé ne peut alors s'opposer à la fouille de ses objets ou de son casier en invoquant la protection de sa vie privée (Pedneault, Bernier et Granosik, 2015, p. 21-137). L'employeur peut lui ordonner de se plier à la fouille. En vertu du droit de l'employeur de commander, le refus constitue un **acte d'insubordination** et peut être sanctionné **par l'employeur** à ce titre.

Cependant, l'employeur ne **peut pas contraindre l'employé à la fouille par la force**, s'il refuse; en effet, il ne s'agit pas d'une arrestation, mais bien d'une vérification de la part de l'employeur, qui n'est pas un représentant des forces de l'ordre (Pedneault, Bernier et Granosik, 2015, p. 21-167). En général, **lorsqu'un employé refuse** d'être fouillé par son employeur, le droit commun s'applique, qui prévoit qu'un citoyen ne fouille pas un autre citoyen.

Dans le contexte où les **employés sont syndiqués**, si la **fouille est plus tard reconnue abusive**, illégale ou injustifiée par le tribunal, et comme les droits fondamentaux de l'employé à la vie privée ont été lésés, un arbitre annulera souvent la sanction disciplinaire. L'employeur doit donc avoir la conviction d'être dans son droit (Pedneault, Bernier et Granosik, 2015, p. 21-167). Le salarié peut même, exceptionnellement, enfreindre la règle suivante : « Obéissez d'abord, déposez un grief ensuite », fréquemment invoquée en droit du travail, car il s'agit d'un droit fondamental. S'il obéit, il abdique de ce fait son droit.

En revanche, toujours dans le contexte où les **employés sont syndiqués**, lorsqu'on **considère que la fouille est justifiée**, le salarié qui a refusé s'expose alors à des sanctions disciplinaires ainsi qu'aux présomptions de fait qu'on peut tirer de son refus (Pedneault, Bernier et Granosik, 2015, p. 21-168). Il risque fort d'être présumé en faute du fait d'avoir refusé.

LES CONDITIONS DE VALIDITÉ D'UNE POLITIQUE DE FOUILLE

Mettre en place une politique : un atout et une assurance

Le droit de l'employeur de procéder à la fouille d'un ordinateur d'un employé dépend de **l'attente de vie privée** de l'employé à l'égard de celui-ci, que le tribunal établit pour chaque cas, à la lumière de l'ensemble des circonstances. Que peut faire l'employeur soucieux d'éviter les mauvaises surprises? **À la lumière de la jurisprudence, la mise en œuvre d'une politique constitue un atout et une assurance.**

La Cour suprême a souligné, dans l'affaire *Cole* (vue plus haut), que **l'adoption de politiques largement diffusées** régissant l'utilisation des appareils électroniques et prévoyant un droit de surveillance de l'employeur avait comme effet de réduire les attentes raisonnables d'un employé en matière de vie privée, sans toutefois les faire disparaître complètement. Cette politique doit satisfaire à certaines conditions pour **demeurer raisonnable et conforme aux droits fondamentaux.**

Réserver les appareils à l'usage professionnel

L'employeur peut se doter d'une politique relative à l'utilisation des ressources

informatiques, qui informe les employés de leurs responsabilités quant à l'utilisation des ressources informatiques de l'entreprise, de leurs obligations, des risques inhérents à un mauvais usage et des conséquences en cas de manquement.

Par exemple, l'employeur est avisé de prévoir que les ressources informatiques doivent être utilisées **exclusivement à des fins professionnelles** et, par conséquent, que l'utilisation d'Internet et du courrier électronique pendant les heures de travail est **limitée aux exigences de l'emploi**. Une telle politique peut notamment servir à démontrer l'usage d'informations confidentielles au détriment de l'employeur (O'Reilly et St-Pierre-Plamondon, 2014, p. 158).

La politique peut, par exemple, préciser que les systèmes informatiques demeurent la propriété exclusive de l'entreprise et que les employés renoncent à toute confidentialité à l'égard de tout ce qu'ils créent, entreposent, envoient ou reçoivent en utilisant les ressources électroniques de l'entreprise ou par Internet durant les heures de travail. Les employés n'ont ainsi plus d'attentes quant au respect de leur vie privée lors de l'utilisation des ressources informatiques de l'employeur ou durant les heures de travail.

Les conséquences de l'autorisation de l'usage personnel

L'employeur peut implanter une politique explicite et bien documentée quant à **l'usage personnel** des appareils : quand et comment il est permis, quelles sont les sanctions, etc.

Cependant, dans l'arrêt *Cole* de la Cour suprême (résumé plus haut), malgré des textes suffisamment clairs selon lesquels le contenu des ordinateurs portables ne doit pas être considéré comme relevant de la vie privée des employés, la Cour suprême a quand même jugé que les employés conservaient une **attente raisonnable en matière de vie privée dès qu'il y avait possibilité d'utiliser un appareil à des fins personnelles**. Les intérêts légitimes de l'employeur peuvent **réduire cette attente, mais pas l'éliminer** (Monet, 2013, p. 45-46).

Seule une politique qui contient une **interdiction formelle de tout usage personnel** de l'appareil, doublée d'une **pratique constante et uniforme** d'interdiction de tout usage personnel, pourrait éliminer toute prétention quant au respect de la vie privée. En revanche, **l'absence de politiques et de procédures** à ce propos renforce et légitime l'attente raisonnable de l'employé en matière de respect de la vie privée (Monet, 2013, p. 46).

L'employeur peut, par sa politique, prévoir que l'utilisation des biens de l'entreprise à des fins personnelles est strictement interdite, à moins d'une autorisation préalable expresse de l'employeur, ce qui réduit l'attente quant à la vie privée de l'employé en cas d'utilisation à des fins personnelles. La politique devrait naturellement prévoir que le matériel demeure la propriété exclusive de l'employeur, ainsi que l'obligation de l'employé de remettre tous les

biens à la fin de l'emploi, d'un contrat ou lors d'une réaffectation. Il est utile d'inclure un rappel à cette fin dans la lettre de fin d'emploi ou de congédiement (O'Reilly et St-Pierre-Plamondon, 2014, p. 159).

La politique devrait prévoir la possibilité pour l'employeur d'imposer des mesures administratives ou disciplinaires, si l'employeur prévoit le faire, et établir clairement son droit de recours pour tous les dommages pouvant résulter d'une infraction à la politique.

Prévoir la possibilité de fouille

Si l'employeur a implanté une politique qui interdit l'usage personnel des ordinateurs, qui précise que l'employeur se réserve le droit de vérifier leur contenu, annonce la possibilité de vérifier les ordinateurs utilisés par ses employés dans certaines situations, avise que de telles vérifications peuvent avoir lieu, et que **cette politique est en vigueur et bien connue des employés autant que de la direction**, les tribunaux tendent à considérer la vérification comme légitime. Cependant, l'employeur doit nourrir un doute raisonnable quant à l'existence d'un comportement déloyal.

À ce sujet, l'employeur qui a adopté une politique est nettement mieux préparé :

- Le fait d'avoir une politique en vigueur et connue de l'employé, qui précise les agissements et les pratiques interdits, par exemple le téléchargement de logiciels interdits et la consultation de matériel pornographique, permet d'établir un motif raisonnable nécessaire et de légitimer la vérification.
- La possibilité pour l'employeur de faire, dans certaines situations, des vérifications des ordinateurs diminue l'attente des employés en matière de protection de la vie privée quant aux informations emmagasinées dans ces ordinateurs et appuie la vérification.

La politique doit être connue de tous

Si l'employeur a une politique concernant la fouille, il doit la respecter à la lettre et veiller à la diffuser. Il doit le faire régulièrement pour que la politique soit valide (Pedneault, Bernier et Granosik, 2015, p. 21-35 et 21-67).

L'application sans discrimination

L'employeur ne doit pas fouiller de façon discriminatoire et ne viser qu'un certain groupe d'employés. En effet, la politique doit s'appliquer sans distinction à tous les employés (Pedneault, Bernier et Granosik, 2015, p. 21-68).

L'employeur doit aussi agir de bonne foi et non de façon abusive (Pedneault, Bernier et Granosik, 2015, p. 21-69). Afin d'éviter des recours de ses employés pour atteinte à leur vie privée, les employeurs devraient préciser dans les contrats d'emploi et dans les politiques et les directives internes :

- quels sont les employés qui ont le droit de vérifier le contenu des ordinateurs d'autres employés;
- quelles sont les catégories d'employés visées par ces vérifications.

Si la politique prévoit la fouille au hasard, l'échantillon des personnes fouillées doit être choisi sans préjugé discriminatoire. L'employeur ou le supérieur doit surveiller ce processus et ne pas laisser un employé choisir lui-même, car il en sera tenu responsable. Un moyen de sélection selon des bâtonnets pigés dans un vase a notamment été reconnue comme non discriminatoire. L'employeur doit être explicite quant au fait que la fouille sera effectuée au hasard et ne pas laisser place à l'interprétation selon laquelle les personnes fouillées sont soupçonnées, lorsque tel n'est pas le cas. La personne qui fouille ne doit pas intimider la personne fouillée. Enfin, la fouille devrait avoir lieu pendant les heures de travail pour éviter que les employés soient « détenus » pendant leurs heures de loisir (Pedneault, Bernier et Granosik, 2015, p. 21-136).

Préciser qui peut fouiller

La politique précise que l'employeur seul peut se réserver le droit de surveiller ou d'autoriser la fouille et de la déléguer à un employé compétent en cette matière.

Dans les contrats que l'employeur a établis avec les fournisseurs de services ou les représentants externes, la politique devrait aussi préciser que ces derniers ne sont pas en droit, de leur propre chef, d'effectuer des vérifications dans les ordinateurs des employés.

Un employeur ne doit pas autoriser un fournisseur de services ou autre représentant externe à effectuer de telles recherches sans avoir obtenu préalablement le consentement d'une personne ayant l'autorité nécessaire dans l'entreprise (Gingras et Gratton, 2014, p. 67-69, citant la décision *Campeau et Services alimentaires Delta Dailyfood Canada inc.* [2012] (CLP)).

RÉFÉRENCES

- Béliveau, Nathalie-Anne et Sébastien Lebel (2011) « Les clauses de non concurrence en matière d'emploi et en matière de vente d'entreprise : du pareil au même? », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de la non concurrence*, vol. 338, Cowansville, Éditions Yvon Blais, p. 113-192
- Bich, Marie-France (2003) « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de la propriété intellectuelle*, vol. 197, Cowansville, Éditions Yvon Blais, p. 243-327
- Commission d'accès à l'information du Québec (CAIQ) *Le courriel électronique*,

http://www.cai.gouv.qc.ca/documents/CAI_FI_courrier_electronique.pdf

Gagnon, Robert P. (2013) *Droit du travail du Québec*, 7^e édition, Cowansville, Éditions Yvon Blais

Gingras, Patrick et Éloïse Gratton (2014) « Accéder ou ne pas accéder au matériel informatique de son employé, telle est la question », *Développements récents en droit du travail*, Service de la formation continue du Barreau du Québec, vol. 383, p. 35-96

<http://edocrtrine.caij.qc.ca/developpements-recents/383/368185469>

Gratton, Éloïse (2013) « Understanding Personal Information: Managing Privacy Risks », LexisNexis, p. 6 et s.

Hébert, Jean-Claude (2013) « Criminalité et vie privée : équilibre fragile – Saisies et fouilles informatiques », dans Congrès annuel du Barreau du Québec, p. 4

http://www.caij.qc.ca/doctrine/congres_du_barreau/2013/25450/index.html

Launay, Dominique et Audrey Dufresne (2008) « L'obligation de non-concurrence lorsque le contrat d'emploi est résilié sans motif sérieux (art. 2095 CcQ) », dans Service de la formation continue du Barreau du Québec, *Développements récents sur la non concurrence*, vol. 289, Cowansville, Éditions Yvon Blais, p. 223-251

Laurier, Justine B. et Tommy Tremblay (2013) « Jurisprudence récente sur les clauses de non-concurrence en matière de contrats de travail et de conventions commerciales », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de la non-concurrence*, vol. 377, Cowansville, Éditions Yvon Blais, p. 3-37

Lefebvre, Sylvain (2008) « Naviguer sur internet: et si on nageait en aux troubles? », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit du travail*, Cowansville, Éditions Yvon Blais, p. 51-128

Lemoine, Jean et Émilie Courchesne Tardif (2011) « Le préjudice du créancier de l'obligation de non concurrence : remèdes et quantification », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de la non concurrence*, vol. 338, Cowansville, Éditions Yvon Blais, p. 193-221

Monet, Dominique (2013) « La détection de la concurrence déloyale dans la foulée de l'arrêt Cole », *Développements récents en droit de la non-concurrence*, Service de la formation continue du Barreau du Québec, vol. 377, p. 41-76

<http://edocrtrine.caij.qc.ca/developpements-recents/377/368159522>

Pedneault, Jean-François, Linda Bernier et Lukasz Granosik (2015) *Les droits de la personne et les relations du travail*, mise à jour 36, mai 2015, Cowansville, Éditions Yvon Blais

Sarrazin, Claude (2007) « La surveillance : quand, comment et pourquoi? », communication présentée au Congrès annuel du Barreau du Québec, Service de la formation continue du Barreau du Québec

<http://edocrtrine.caij.qc.ca/congres-du-barreau/2007/1731858309>

