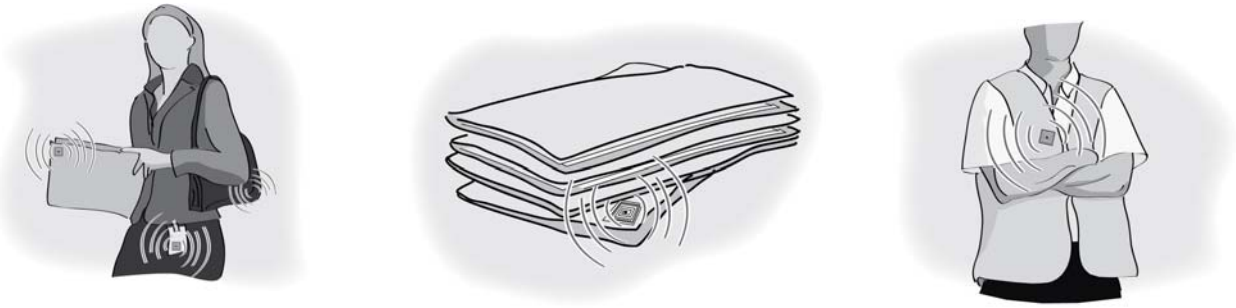
Commissariat à la
protection de la vie privée
du Canada

Office of the
Privacy Commissioner
of Canada



L'identification par radiofréquence (IRF) en milieu de travail : Recommandations de règles de pratique

Document de consultation

Mars 2008

L'identification par radiofréquence (IRF) en milieu de travail : Document de consultation sur les recommandations de règles de pratique

Table des matières

Résumé

La commissaire à la protection de la vie privée du Canada a produit ce document de consultation afin d'établir des règles de pratique à l'intention des organisations qui cherchent à tirer le meilleur parti des technologies d'identification par radiofréquence (IRF). Bien que l'IRF puisse servir de soutien à de nombreuses applications possibles destinées à plusieurs secteurs et activités, le présent document porte sur l'utilisation de l'IRF en milieu de travail. La commissaire craint que les systèmes d'IRF ne servent de dispositifs de surveillance, ce qui compromettrait grandement la dignité et l'autonomie des employés. Le message principal de ce document est que le déploiement de ces technologies en milieu de travail, le cas échéant, doit être effectué de manière à protéger la vie privée et conformément aux principes relatifs à l'équité dans le traitement de l'information.

Dans ce document, on reconnaît qu'il existe déjà un éventail d'usages réels et projetés de l'IRF en milieu de travail. La technologie d'IRF peut servir à effectuer le suivi d'outils, d'équipement ou d'un inventaire, à surveiller l'accès à des installations ou à des zones sécurisées, ou à observer le déroulement d'activités. Les systèmes d'IRF peuvent également être conçus de manière à améliorer la sécurité et la sûreté. Bien que les employés puissent tirer avantage de certaines utilisations de l'IRF, la présence de cette technologie en milieu de travail soulève d'importants enjeux liés à la vie privée des employés. Par exemple, ce sont des personnes qui, la plupart du temps, se servent des outils et de l'équipement, et qui déplacent l'inventaire; par conséquent, leurs mouvements et leur productivité pourraient faire l'objet d'une surveillance plus étroite.

La partie I de ce document offre un aperçu de la technologie d'IRF et des risques en matière de sécurité et de protection de la vie privée liés à l'utilisation des systèmes d'IRF en général. Les personnes qui connaissent déjà la technologie d'IRF gagneraient toutefois à lire le résumé des risques envers la vie privée et la sécurité proposé dans cette section, puisqu'il sert de fondement aux prises de position adoptées dans les deuxième et troisième parties du document.

La partie II présente la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*)[1] et la *Loi sur la protection des renseignements personnels*[2], et aborde différentes manières par lesquelles les renseignements compris dans une étiquette d'IRF peuvent devenir des renseignements personnels. On aborde également dans cette partie les attentes raisonnables en matière de protection de la vie privée en milieu de travail, et l'on fait référence à diverses conclusions et à des dossiers judiciaires pertinents.

Le document énumère ensuite les mesures que les organisations devraient adopter ainsi que les questions qu'elles doivent se poser avant d'introduire des applications d'IRF en milieu de travail. Dans certains cas, l'employeur pourrait conclure, avec raison, que les coûts entraînés par certaines applications sont plus importants que les avantages qui peuvent en découler. Aux entreprises qui décident d'aller de l'avant, la commissaire suggère des pratiques exemplaires fondées sur les principes relatifs à l'équité dans le traitement de l'information.

La partie III comprend une série de questions auxquelles nous espérons recevoir des réponses; nous apprécierons toutefois recevoir des commentaires au sujet de tout élément soulevé dans le présent

document. Nous espérons tout particulièrement recevoir les commentaires de ceux qui peuvent être touchés directement par l'IRF en milieu de travail, soit les employeurs, les employés et les syndicats, ainsi que les développeurs de technologie d'IRF.

Public cible

Ce document de consultation a été rédigé à l'intention d'un vaste auditoire. Il s'adresse aux employeurs qui prévoient utiliser ou qui utilisent déjà la technologie d'IRF pour suivre les déplacements de leurs employés ou de leurs biens, mais aussi aux employés et aux syndicats, afin de les sensibiliser davantage à ces enjeux. Eu égard à son auditoire, ce document évite le vocabulaire technique lorsqu'il n'est pas nécessaire. Toutefois, ce document de consultation a également été élaboré afin d'encourager les fournisseurs d'IRF à faire preuve d'une plus grande responsabilité à l'égard des produits qu'ils conçoivent. Nous sollicitons la rétroaction de tous ces groupes et de toute autre partie intéressée, afin de clarifier les recommandations de pratiques exemplaires formulées ici.

Portée et structure du document de consultation

Bien que l'IRF puisse servir de soutien à de nombreuses applications destinées à plusieurs secteurs et activités, le présent document porte sur l'utilisation de l'IRF en milieu de travail. En diffusant le présent document de consultation, la commissaire à la protection de la vie privée ne veut aucunement laisser entendre qu'elle ferme les yeux — ou qu'elle jette le blâme — sur l'utilisation de la technologie d'IRF pour suivre le déplacement des employés. Son objectif est d'établir des règles de pratique solides afin que les technologies en question soient déployées de manière à respecter la vie privée et conformément aux principes relatifs à l'équité dans le traitement de l'information. La mise sur pied d'un environnement de travail qui respecte la dignité et l'autonomie des employés est une responsabilité que se partagent les employeurs, les employés et les syndicats.

Ce document comprend trois parties. La partie I offre un aperçu de la technologie d'IRF et des risques en matière de sécurité et de protection de la vie privée liés à l'utilisation des systèmes d'IRF en général. On y examine aussi l'état actuel de la technologie, et l'on tente de prévoir son évolution et les répercussions qu'elle pourrait avoir sur le droit à la vie privée dans le contexte précis du milieu de travail.

La partie II présente la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*)[3] et la *Loi sur la protection des renseignements personnels*[4]. On y présente l'avis du Commissariat à la protection de la vie privée concernant les règles de pratique relatives à l'utilisation des systèmes d'IRF en milieu de travail en conformité avec la *LPRPDÉ* et la *Loi sur la protection des renseignements personnels*.

La partie III comprend une série de questions auxquelles nous espérons recevoir des réponses.

En 2005, le Commissariat à la protection de la vie privée du Canada a écrit à plusieurs grandes sociétés canadiennes susceptibles d'utiliser l'IRF dans le cadre de leurs activités commerciales. Nous leur avons demandé de nous aider à comprendre l'utilisation croissante de l'IRF au Canada[5]. Un seul organisme a affirmé qu'il utilisait l'IRF pour suivre le déplacement de ses employés, mais il s'agissait d'un cas révélateur auquel il nous semblait important de donner suite.

L'organisme nous a expliqué que tous ses employés transportent des appareils d'accès contenant des dispositifs d'IRF actifs ou passifs. Ces mécanismes contrôlent l'utilisation de certains appareils, comme les chariots élévateurs. L'organisme conserve des relevés de l'utilisation de ces dispositifs dans les cas, entre autres, d'accès non autorisés à des zones réservées ou à certains appareils. Il surveille aussi les activités de certains employés afin de déterminer le temps qu'ils consacrent à chaque activité et leur assiduité. Les responsables de l'organisme ont affirmé que, selon eux, il ne s'agissait pas d'une collecte de renseignements personnels.

Rien dans le présent document ne doit être perçu comme un obstacle ou une entrave à l'exercice du pouvoir discrétionnaire du Commissariat à la protection de la vie privée du Canada dans le cadre de ses responsabilités, particulièrement en ce qui concerne les plaintes déposées par des personnes au titre de la *LPRPDÉ* ou de la *Loi sur la protection des renseignements personnels*.

Les règles de pratique visant l'utilisation de l'IRF en milieu de travail proposées dans le présent document pourraient être révisées à mesure que l'on en apprend davantage sur l'incidence de la technologie d'IRF sur la protection de la vie privée. Les règles de pratique seront mises à jour pour tenir compte des progrès technologiques et des nouvelles applications d'IRF.

Introduction

> *[...] la vie privée constitue une valeur démocratique essentielle, car s'il est impossible de protéger le domaine personnel, il sera beaucoup moins probable que nous puissions exercer nos autres droits.*[6]
> — M[me] Valerie Steeves, professeure, devant le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie à propos du projet de loi S-21 qui vise à garantir le droit des personnes à la vie privée, 20 septembre 2001.

La commissaire à la protection de la vie privée du Canada a pour mission de promouvoir le droit à la vie privée. En plus d'enquêter sur des plaintes et de mener des vérifications, elle est habilitée à publier de l'information sur les pratiques relatives au traitement des renseignements personnels dans les secteurs public et privé, à effectuer des recherches sur des enjeux liés à la protection de la vie privée, et à faire mieux connaître et comprendre à la population canadienne les enjeux concernant la protection de la vie privée.

La commissaire surveille depuis un certain temps l'évolution des applications de l'identification par radiofréquence (IRF) et a fait état de ses préoccupations touchant cette technologie, notamment en ce qui concerne l'identification de personnes, dans ses rapports annuels au Parlement. Selon elle, l'IRF pourrait avoir de graves conséquences en matière de protection de la vie privée et il faudrait donc dès maintenant établir des règles de pratique à l'intention des organismes visés par la *LPRPDÉ* et la *Loi sur la protection des renseignements personnels*. Si l'IRF peut s'appliquer à une vaste gamme de secteurs et d'activités, le présent document porte particulièrement sur l'utilisation de l'IRF en milieu de travail.

On recense déjà diverses façons d'utiliser l'IRF en milieu de travail et d'autres utilisations sont envisagées. La technologie de l'IRF permet, par exemple, d'effectuer le suivi d'outils, d'appareils ou d'articles en inventaire, de surveiller l'accès à des installations ou à des zones protégées, ou d'obtenir une vue d'ensemble des modèles d'activités. Les systèmes d'IRF peuvent aussi être conçus de façon à renforcer la protection et la sécurité. Si l'IRF peut, dans certains cas, présenter des avantages pour les employés, le recours à l'IRF en milieu de travail suscite aussi des préoccupations importantes en matière de protection de la vie privée des employés. D'autres études et lignes directrices devront porter officiellement sur ces préoccupations. On ne connaît pas encore la nature et l'étendue des utilisations possibles de l'IRF en milieu de travail, mais il est tout de même opportun de formuler des règles de pratique dès maintenant.

La commissaire reconnaît que, comme c'est le cas pour toute nouvelle technologie, les applications et les capacités de l'IRF peuvent évoluer à une vitesse extraordinaire, ce qui fait qu'il est difficile d'en prévoir avec précision les répercussions. En conséquence, on ne se contente pas, dans le présent document, d'établir une série de règles de pratique pour l'utilisation de l'IRF en milieu de travail; on fait également appel à des commentaires sur l'application, à la technologie de l'IRF en milieu de travail, des principes relatifs à l'équité dans le traitement de l'information, par le truchement d'une série de questions figurant à la fin de la partie III.

Comme pour toute technologie, il faut absolument régler les problèmes de protection de la vie privée liés à la technologie de l'IRF avant son déploiement, de façon à ce que les employeurs puissent déterminer s'il est opportun ou nécessaire de faire appel à la technologie d'IRF. Les concepteurs de systèmes sont donc forcés d'inclure aux nouvelles technologies des fonctions de protection de la vie privée pour répondre aux exigences de leurs clients. De plus, les employés et les syndicats qui les

représentent ont ainsi l'occasion de jouer un rôle actif dans la prise de décisions concernant la mise en place de nouveaux systèmes de surveillance en milieu de travail. Cette façon de procéder permet d'établir des règles de pratique avant que des pratiques non respectueuses de la vie privée soient adoptées. Elle permet également de reconnaître les systèmes qui ne devraient pas être déployés.

La protection de la vie privée est étroitement liée à la dignité humaine et à l'autonomie. Bon nombre de Canadiennes et de Canadiens passent beaucoup de temps au travail. On doit absolument porter attention à la possibilité que la technologie de l'IRF permette une surveillance accrue en milieu de travail. Si l'on veut protéger la dignité humaine en milieu de travail, il faut utiliser ces technologies de façon à respecter la vie privée.

PARTIE I – L'IRF : Enjeux relatifs à la protection de la vie privée et risques pour la sécurité

1. Qu'est-ce que l'IRF?

> *Les technologies les mieux enracinées sont celles qui disparaissent. Elles se fondent dans l'essence même du quotidien jusqu'à en devenir indissociables* [traduction].[7]
> — Mark Weiser, « The Computer for the 21st Century »

Dans les paragraphes qui suivent, on décrit de façon très générale la technologie d'IRF. L'annexe I du présent document fournit de plus amples détails sur le fonctionnement de l'IRF et l'annexe II comprend une bibliographie d'ouvrages à consulter.

Le terme IRF est un terme générique employé généralement pour décrire les technologies qui permettent de stocker des données sur de petites puces, ou étiquettes, et de les transmettre à distance à un lecteur par l'entremise de la radiotransmission. La technologie compte trois composantes de base : l'étiquette d'IRF en tant que telle (composée d'une antenne jointe à une puce), le lecteur d'IRF et l'infrastructure de la base de données connexe (matérielle et logicielle). La définition de l'IRF doit demeurer générale puisque les capacités techniques de la RF et les distinctions entre les technologies de RF évolueront au fil du temps[8].

La technologie d'IRF se distingue par le fait que les étiquettes peuvent être lues même en l'absence de visibilité directe et à travers des matériaux durs comme la couverture d'un livre ou un matériau d'emballage. De plus, il est possible de lire plus d'une étiquette à la fois. Chaque étiquette permet d'identifier l'objet précis auquel elle est fixée, même si celui-ci se trouve au milieu d'une multitude d'objets identiques. Avec la technologie des codes à barre, par exemple, le code à barre d'une bouteille d'eau est le même que celui de toutes les autres bouteilles d'eau de la même marque. La technologie d'IRF permet d'attribuer un identificateur distinct à chaque bouteille d'eau.

L'IRF fait partie d'un ensemble de technologies dont la complexité et les capacités varient grandement. Par exemple, les étiquettes des chaînes d'approvisionnement, que l'on appelle étiquettes de code électronique de produit (code EPC), doivent être simples, peu coûteuses et jetables. Afin que leur coût demeure le plus bas possible, les étiquettes EPC ne peuvent emmagasiner que très peu de données dans leur mémoire intégrée. Par opposition, certaines étiquettes peuvent emmagasiner une quantité importante de données, y compris des données biométriques[9].

D'autres technologies de RF plus complexes, comme les cartes sans contact ou « cartes à puce », offrent potentiellement des couches de sécurité supplémentaires[10]. Les promoteurs de la technologie des cartes sans contact prétendent qu'il s'agit d'une technologie beaucoup plus complexe. Par exemple, dans le cas des applications qui permettent un accès par carte sécurisée, le dispositif doté d'une carte à puce sans contact peut vérifier l'authenticité du lecteur et prouver sa propre authenticité à celui-ci avant le début d'une transaction sécurisée[11]. De plus, il est possible de chiffrer l'information qui circule entre le dispositif à carte à puce sans contact et le lecteur afin d'éviter son interception non autorisée. Pourtant, du point de vue des employés et sur le plan de la protection de la vie privée en milieu de travail, les enjeux de protection de la vie privée liés aux étiquettes d'IRF et aux cartes à puce

sont essentiellement les mêmes. Bien que les cartes à puce puissent améliorer la sécurité et l'authentification, les règles de pratique énoncées dans le présent document s'appliquent à la collecte de renseignements personnels tant à l'aide de l'IRF qu'au moyen des cartes à puce, puisque toutes deux mettent en jeu la protection de la vie privée.

Les dispositifs qui utilisent les fréquences radioélectriques ne font pas tous partie de la technologie d'IRF. Par exemple, les dispositifs antivol fixés aux biens de consommation que l'on trouve dans les magasins fonctionnent grâce aux fréquences radioélectriques, mais ne contiennent pas les identificateurs uniques qui font partie intégrante de la technologie d'IRF.

Les capteurs font aussi partie de la famille des dispositifs sans fil de RF. Il s'agit de petits dispositifs matériels qui réagissent à des stimuli physiques et produisent un signal électronique, tout comme les étiquettes d'IRF, transmettant de l'information sur leur environnement comme sur le mouvement, la lumière, la température ou l'humidité. Les capteurs contiennent habituellement des piles et peuvent avoir les mêmes applications que les étiquettes d'IRF les plus complexes, par exemple pour détecter si un conteneur dont l'accès est protégé a été ouvert[12].

Il existe aussi des systèmes d'IRF « sans puce », dans lesquels de minuscules particules chimiques ayant divers degrés de magnétisme réagissent quand elles sont sollicitées par un lecteur. Cette technologie de RF pourrait, entre autres, permettre d'incorporer les particules à du papier ou de les imprimer sur du papier, et de placer des lecteurs dans les photocopieurs de façon à empêcher les copies non autorisées[13].

Les règles de pratique énoncées dans le présent document s'appliquent dans tous les cas où l'une ou l'autre de ces technologies est employée en milieu de travail pour surveiller les activités ou les déplacements d'employés ou pour recueillir des données sur des employés identifiables.

2. L'IRF en milieu de travail

> *La protection de la vie privée en milieu de travail est une composante importante des droits fondamentaux à l'autonomie des personnes dans notre société. Les gens passent une bonne partie de leur vie au travail. Or, ce qui se produit au travail — y compris la protection de la vie privée — peut avoir un effet marqué sur le sentiment de dignité, de liberté et d'autonomie des employés. La surveillance continuelle est déshumanisante. Elle n'aide pas à créer un milieu de travail agréable.*[14]
> — Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, le 30 novembre 2006.

Les gens s'attendent à jouir d'une certaine intimité au travail, même s'ils se trouvent dans les installations de l'employeur et qu'ils utilisent son équipement. En même temps, il est normal que l'on doive renoncer un peu à sa vie privée quand on travaille pour quelqu'un. Les employeurs ont besoin de renseignements de base sur leurs employés, par exemple en ce qui concerne la paye et les avantages sociaux, et ils doivent être en mesure de s'assurer que le travail est effectué de façon sûre et efficace[15].

La surveillance des employés et de leurs activités peut toutefois devenir excessive et mener à une ingérence inacceptable dans leur vie privée. Une telle ingérence a des répercussions sur la dignité et l'autonomie de l'employé. Aujourd'hui, les possibilités de porter atteinte à la vie privée en milieu de travail sont plus nombreuses que jamais. On peut penser aux tests psychologiques, aux relevés des sites Web visités, à la surveillance vidéo, à la surveillance de la frappe, aux tests génétiques et aux

systèmes mondiaux de localisation, mais aussi à l'IRF, qui est un outil supplémentaire dont disposent les employeurs pour surveiller les employés dans l'exercice de leurs fonctions. Comme la mise en place de systèmes d'IRF coûte de moins en moins cher d'année en année, les organismes pourraient choisir d'utiliser de tels systèmes pour effectuer un suivi de la productivité, améliorer la sécurité et réduire le vol[16]. Il y a également le risque que les employés disposant d'un appareil d'IRF et de pièces d'identité fassent l'objet d'une surveillance à l'extérieur du milieu de travail.

On peut reconnaître que la technologie des systèmes d'IRF présente des avantages pour les employeurs et même, dans certains cas, pour les employés, mais on ne devrait pas pour autant renoncer à la protection de la vie privée des employés. Le CPVP a décidé de produire le présent document parce qu'il est convaincu que le fait d'agir de façon proactive relativement à la conception et au déploiement de nouvelles technologies peut favoriser la protection de la vie privée, puisque cela permet de garantir une conception et un déploiement consciencieux et appropriés des technologies de manière à anticiper les problèmes de protection de la vie privée et à les régler.

La commissaire s'inquiète des résultats publiés dans un rapport au sujet de l'IRF en milieu de travail émis par la société RAND en 2005[17]. Le rapport portait sur six grands organismes du secteur privé des États-Unis. Les auteurs du rapport ont constaté que certains employeurs utilisaient déjà la technologie d'IRF pour surveiller leurs employés, et que les organismes ne disposaient d'aucune politique pour régir ces activités. Ils ont formulé, entre autres, les constatations suivantes :

- Tous les organismes affirmaient qu'il existait des liens entre les données recueillies à l'aide du système de contrôle de l'accès utilisant l'IRF et d'autres bases de données (si on utilisait le nom de l'employé ou un autre identificateur). Dans tous les cas, les données recueillies étaient liées aux données figurant dans les dossiers personnels et, dans un cas, elles étaient liées à des renseignements médicaux relatifs aux allergies.

- Aucun des organismes visés par l'étude n'avait établi de politique de conservation des données et tous conservaient les données sur le contrôle d'accès pour une période indéterminée. Un seul organisme disposait d'un énoncé de politique à l'échelle de l'entreprise décrivant les normes de conservation et d'utilisation des données recueillies par le système de contrôle de l'accès, mais cet énoncé n'était remis qu'à certains employés[18].

Si l'on avait agi de façon proactive relativement à la protection de la vie privée au moment d'adopter et de mettre en œuvre la technologie d'IRF dans ces cas, cette technologie aurait probablement été déployée d'une toute autre façon.

L'IRF est déjà utilisée dans certains milieux de travail. Par exemple :

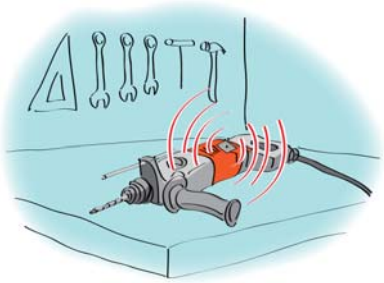
- IBM met actuellement en marché un système qui utilise une étiquette d'IRF intégrée dans des insignes d'identité personnalisés. Les récepteurs répartis sur le site reçoivent le signal unique transmis par chaque étiquette et le système repère l'emplacement exact de l'étiquette à ce moment précis[19].

- Un casino de Sydney, en Australie, se sert de l'IRF pour gérer son stock, comprenant plus de 80 000 uniformes, dont la valeur atteint presque deux millions de dollars US. Pour régler ses problèmes de buanderie, le casino attache une étiquette d'IRF à chaque uniforme et des lecteurs placés à des endroits stratégiques permettent au système de suivre les uniformes[20].

- En juillet 2005, le syndicat GMB, l'un des plus importants du Royaume-Uni, exigeait l'abandon de la surveillance par l'IRF des employés des épiceries de l'Europe, proclamant qu'il s'agissait d'une atteinte à la vie privée des travailleurs. On avait demandé aux travailleurs de porter de petits ordinateurs au poignet, au bras et au doigt afin que l'on puisse leur dire quoi faire et où aller[21].

Si la lecture d'une étiquette d'IRF attachée à un objet ou à un outil en milieu de travail se fait en même temps que celle d'un autre dispositif à puce comme la carte d'identification d'un employé, la surveillance des employés pourrait être sans limites. Comme le souligne M^me^ Perrin :

> [. . .] *la gestion des stocks d'outils coûte très cher à bon nombre d'industries de services; les outils qui gardent une trace des endroits où ils sont allés et de leurs utilisations pourraient connaître un grand succès. On pourrait juger que la valeur de la surveillance des outils dépasse celle de la dignité des employés qui utilisent ces outils* [traduction][22].



Dans le contexte du milieu du travail, on peut décider d'adopter un système d'IRF explicitement dans le but de surveiller les déplacements des employés. Certaines entreprises procèdent déjà à des expériences plutôt complexes de surveillance des biens et des employés à l'aide de l'IRF. Par exemple, IBM participe à un projet pilote avec une grande société pétrochimique, présente partout dans le monde, pour mettre à l'essai un système élaboré de surveillance des biens et de reconnaissance de l'emplacement. Les partenaires ont approuvé des plans qui prévoient l'ajout d'autres emplacements. Le système inclut :

- des étiquettes d'IRF actives que portent les employés travaillant dans un milieu stratégique;
- des récepteurs qui permettent de détecter les étiquettes d'IRF à chaque point d'entrée d'une installation et de connaître en tout temps l'emplacement des employés en temps réel virtuel;
- des mises à jour automatiques à partir des systèmes de ressources humaines permettant de vérifier les accréditations des employés et les autorisations d'accès à des zones réglementées;
- des alertes qui signalent la violation d'une zone de sécurité[23].

Des dispositifs complexes et coûteux, qui combinent la technologie d'IRF et celle du système mondial de localisation (GPS), peuvent fournir en continu des données géographiques assez précises. Si l'on peut associer en plus une étiquette à une personne, on peut donc suivre ses déplacements. Par exemple, un système d'étiquettes GPS, proposé pour assurer le suivi de l'équipement des travaux publics de la Ville de Montréal, a été perçu par certains comme une façon indirecte de surveiller les habitudes de travail des employés municipaux[24].

On a aussi envisagé l'utilisation des étiquettes IRF pour les employés dont les tâches présentent des risques élevés, comme les pompiers ou les soldats. Grâce aux étiquettes, on peut avoir accès rapidement aux renseignements médicaux et d'identification de personnes gravement blessées ou inconscientes[25].

Ces exemples nous donnent un aperçu des répercussions sur le droit à la vie privée des employés que peuvent avoir l'adoption et la mise en œuvre de systèmes d'IRF en milieu de travail. On décrit plus en détail ci-dessous les effets possibles sur la protection de la vie privée.

3. L'IRF et les risques d'atteinte à la vie privée

Les systèmes d'IRF soulèvent de nouveaux risques envers la vie privée qui viennent s'ajouter à ceux qui découlent d'autres formes de surveillance des activités des employés comme la vidéo et la reconnaissance de la frappe au clavier. Parce qu'elle comprend à la fois l'emplacement géographique, la date et l'heure, la surveillance par IRF en milieu de travail permet d'automatiser la surveillance des employés et d'avoir un portrait précis de leur interaction avec les autres employés. Plus on surveille les employés, plus on porte atteinte à leur vie privée et, au bout du compte, à leur dignité et à leur autonomie au travail.

Certains risques, bien qu'ils soient aussi associés à d'autres technologies de surveillance, sont particulièrement importants dans le cas de l'IRF. On les décrit dans les pages qui suivent.

3.1. Collecte secrète de renseignements personnels

La technologie d'IRF peut être employée partout. Les étiquettes d'IRF sont petites et peuvent être intégrées à des objets et à des documents à l'insu de la personne qui les obtient. Les travaux de recherche visant à réduire la taille des étiquettes progressent rapidement. Par exemple, Hitachi annonçait il y a quelques années la puce-mu, une étiquette passive très petite (moins de 0,4 mm), qui pourrait être fixée à du papier de façon à repérer des documents[26]. Récemment, l'entreprise a conçu la « poussière » d'IRF, beaucoup plus petite que la puce-mu et qui pourrait être utilisée à des fins semblables[27]. Eastman Kodak travaille même à mettre sur pied une étiquette d'IRF ingérable qui pourrait être intégrée aux médicaments[28].

Comme les ondes radio se déplacent facilement et en silence, qu'elles traversent le tissu, le plastique et d'autres matériaux et qu'elles n'exigent pas de visibilité directe, il est possible de lire les étiquettes d'IRF cousues dans un vêtement comme un uniforme, ou fixées à un objet rangé dans une poche, un sac à main, un sac à dos ou tout autre endroit. Pour lire les étiquettes à distance, des lecteurs peuvent être intégrés de façon invisible à presque n'importe quel environnement où se trouvent des êtres humains ou des objets. Il est possible de lire une étiquette à une distance plus longue que prévue si l'on augmente la portée d'un lecteur. On ne peut donc pas toujours savoir d'emblée que l'IRF est utilisée, ce qui signifie qu'il est virtuellement impossible pour une personne de savoir si un objet en sa possession ou elle-même fait l'objet d'une surveillance. Ainsi, selon la façon dont l'IRF est utilisée dans un milieu de travail, il se peut que des employés ne sachent pas du tout qu'on les surveille, ou qu'ils ne sachent pas dans quelle mesure on le fait.

Il peut aussi arriver que des étiquettes d'IRF installées par un organisme soient « lues » par des lecteurs non autorisés. Cela signifie que les activités et les emplacements des employés qui portent une étiquette d'IRF peuvent être surveillés par quelqu'un d'autre que leur employeur, peut-être à des fins illégales ou dangereuses[29].

Les percées technologiques, particulièrement en matière de nanotechnologie, peuvent élargir la capacité d'exercer de la surveillance clandestine. Alors que nous atteignons les limites physiques des capacités de stockage et de traitement des ordinateurs d'aujourd'hui, la nanotechnologie nous permettra de concevoir des appareils de traitement et de détection infiniment plus petits et beaucoup plus puissants. Ces appareils pourraient être dispersés un peu partout dans notre environnement et être invisibles à l'œil nu.[30]

3.2 « Détournement d'usage » et utilisations secondaires

Les raisons pour lesquelles un système d'IRF est, au départ, mis en place dans un milieu de travail peuvent évoluer au fil du temps et entraîner une surveillance et un suivi accrus des personnes et de leurs activités. Par exemple, l'aéroport international d'Helsinki utilisait initialement la technologie d'IRF pour consigner les heures de travail du personnel au sol. En 2006, les responsables de l'aéroport annonçaient qu'ils utiliseraient désormais l'IRF pour effectuer en plus un suivi de toutes les tâches du personnel au sol[31].

De plus, d'autres personnes pourraient tenter d'obtenir des données recueillies à l'aide de l'IRF à des fins non liées à l'emploi. Par exemple, les relevés des dispositifs d'IRF (sous forme de transpondeurs) dont se servent les automobilistes pour passer les postes à péage ont déjà été utilisés dans le règlement du divorce de certains automobilistes comme preuve d'infidélité. Ces relevés peuvent aider à déterminer où se trouvait la voiture d'une personne à un moment précis[32].

Les renseignements recueillis en milieu de travail à des fins de surveillance des stocks ou de l'équipement et liés à des personnes identifiables pourraient être aussi utilisés à des fins disciplinaires envers un employé, voire à des fins d'enquête criminelle ou de poursuite.

En outre, les ministères et organismes gouvernementaux pourraient souhaiter avoir accès aux données détenues par les organismes à diverses fins, y compris en cas d'enquête criminelle ou de menace pour la sécurité nationale, ou pour l'application de la loi. Il serait également possible d'utiliser des données obtenues par des dispositifs d'IRF pour surveiller les déplacements de personnes liées à des causes politiques impopulaires.

4. L'IRF et les risques pour la sécurité

On a cerné plusieurs risques pour la sécurité associés à l'IRF[33].

- Falsification du contenu des étiquettes : S'il est impossible d'écraser des données dans des étiquettes d'IRF non inscriptibles, plus difficiles à corrompre, on peut facilement modifier le contenu d'une étiquette inscriptible non protégée. Par exemple, un pirate pourrait saisir les données qui se trouvent dans une étiquette associée à un objet, puis les copier dans l'étiquette d'un autre objet.

- Manipulation physique : Une étiquette pourrait être retirée d'un article pour être fixée à un autre. Par exemple, une étiquette d'IRF fixée à un ordinateur portatif contenant des renseignements de nature délicate pourrait être laissée sur un bureau ou fixée à un autre objet. Dans le cas d'une étiquette d'IRF intégrée à l'insigne nominatif ou à l'uniforme d'un

employé, une personne autre que l'employé pourrait utiliser l'insigne ou l'uniforme, ce qui fournirait des données erronées sur les déplacements ou les activités de l'employé.

- Clonage : Un voleur de données pourrait se servir d'un dispositif de clonage sans fil pour saisir les données contenues dans une étiquette. Par exemple, un voleur pourrait cloner, dans un stationnement, la carte d'accès d'un employé utilisant l'IRF, ce qui lui permettrait d'entrer dans le lieu de travail sans autorisation. Des voleurs ont déjà réussi, à la suite d'attaques musclées, à s'emparer des données contenues dans des étiquettes plus complexes utilisant le chiffrement. Des voleurs ont même réussi à cloner des étiquettes d'IRF implantables et ont utilisé ces renseignements pour accéder à tous les documents auxquels l'étiquette était associée, dont des dossiers médicaux[34].

- Interception illicite : Un tiers peut capter clandestinement les transmissions d'un dispositif d'IRF et ainsi recueillir les données que l'employeur souhaite enregistrer.

- Retransmission : Un voleur peut intercepter une transmission valide puis la transmettre de nouveau.

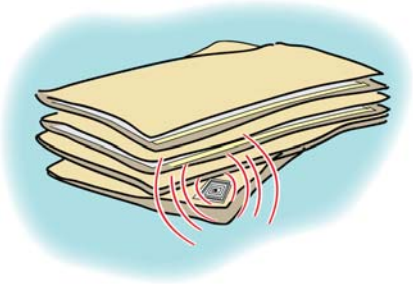
- Infection des étiquettes : Des chercheurs ont découvert une façon de contaminer des étiquettes d'IRF par l'entremise de vers informatiques, ce qui signifie que les produits et les cartes d'identification pourraient servir à propager un code destructeur[35].

La plupart de ces risques pour la sécurité ont surtout des répercussions directes sur les activités commerciales de l'organisme, mais elles peuvent aussi avoir des répercussions sur les employés. Un employé pourrait être pris à partie pour des actes commis par un tiers qui se serait approprié ou aurait utilisé illégalement son étiquette ou une carte à puce, l'examen des relevés donnant à penser que l'employé aurait accédé illégalement à une zone à accès restreint, aurait été le dernier à utiliser un appareil manquant, etc.

Diverses méthodes permettent de régler les problèmes de sécurité liés à l'IRF, y compris des politiques, des processus et des technologies. Il est, de toute évidence, préférable de régler les questions de sécurité et de protection de la vie privée avant l'adoption et le déploiement de cette technologie, que ce soit à l'aide de politiques, de processus ou de technologies. Dans certains cas, ces risques peuvent être contournés en n'utilisant tout simplement pas de dispositifs adaptés à l'IRF.

On confond souvent les termes de sécurité et de protection de la vie privée. Les lois relatives à la protection de la vie privée exigent certainement une sécurité adéquate des données, puisque des données ou des systèmes non protégés peuvent entraîner des risques importants pour la protection de la vie privée. Cependant, le simple fait pour un organisme de garantir la collecte, l'utilisation et la communication protégées des données ne signifie pas qu'il respecte ses obligations juridiques en matière de protection de la vie privée. La collecte, l'utilisation et la communication de renseignements personnels doivent se faire dans le respect des principes relatifs à l'équité dans le traitement de l'information, lesquels sont enchâssés dans les lois sur la protection des renseignements personnels.

PARTIE II – Les règles de pratique relatives aux dispositifs d'IRF en milieu de travail : Respect de la législation canadienne en matière de protection des renseignements personnels



Au Canada, les organismes qui utilisent l'IRF n'ont pas l'obligation explicite d'informer les personnes de la présence de la technologie, de la raison pour laquelle ils l'utilisent et de la façon dont l'information recueillie sera employée. Cependant, quand un organisme recueille des renseignements personnels, les lois visant la protection des renseignements personnels s'appliquent. En outre, quand les données recueillies, utilisées ou communiquées à l'aide d'un système d'IRF concernent une personne, on doit tenir compte des enjeux liés à la protection de la vie privée. Selon la nature du milieu de travail, les normes énoncées dans la *LPRPDÉ* ou dans *Loi sur la protection des renseignements personnels* peuvent s'appliquer. Dans la présente partie, on décrit plus en détail ces lois et leur application.

1. Le secteur public fédéral – La *Loi sur la protection des renseignements personnels*

La *Loi sur la protection des renseignements personnels*, qui s'applique au secteur public fédéral[36], fournit des balises pour l'utilisation de l'IRF au sein du secteur public. Par exemple, les articles 4 à 8 de la *Loi sur la protection des renseignements personnels* établissent le cadre des activités du gouvernement fédéral en ce qui a trait à la collecte, l'utilisation et la communication des renseignements personnels. Il existe des politiques du Conseil du Trésor régissant la gestion des fonds de renseignements personnels[37], la *Politique sur la sécurité du gouvernement*[38], le *Code de la protection des renseignements personnels concernant les employés*[39] et la *Politique d'évaluation des facteurs relatifs à la vie* privée du Conseil du Trésor[40]. L'Évaluation des facteurs relatifs à la vie privée est un processus permettant aux organisations de déterminer si une nouvelle technologie ou initiative, ou un nouveau système d'information respectent les exigences de base en matière de protection de la vie privée.

Le droit à la vie privée serait mieux protégé par la *Loi sur la protection des renseignements personnels* si cette dernière était mise à jour de façon à tenir compte de l'utilisation croissante de ce type de technologie. La *Loi sur la protection des renseignements personnels* n'a pas fait l'objet de modifications importantes depuis son entrée en vigueur en 1983, soit bien avant que les ordinateurs personnels, Internet, les communications sans fil et les autres technologies de l'information et des communications ne révolutionnent la société canadienne. En juin 2006, la commissaire présentait au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique un rapport dans lequel elle décrivait des réformes possibles de la Loi.

En plus de la *Loi sur la protection des renseignements personnels*, que doivent respecter les établissements fédéraux, il existe des critères plus exhaustifs, fondés sur la *LPRPDÉ*, que le Conseil du Trésor a établis dans le cadre du processus d'Évaluation des facteurs relatifs à la vie privée. Les établissements fédéraux doivent considérer ces critères fondés sur la *LPRPDÉ* comme des moyens d'améliorer leurs pratiques de traitement de l'information.

Compte tenu de l'importance accordée aux critères fondés sur la *LPRPDÉ* dans les documents du Conseil du Trésor, le Commissariat est d'avis qu'il est pertinent d'aborder la question de l'application de la *LPRPDÉ* à l'utilisation de l'IRF par des organismes régis par la *Loi sur la protection des renseignements personnels*.

2. Le secteur privé fédéral – La *LPRPDÉ*

La *LPRPDÉ* s'applique aux renseignements personnels recueillis, utilisés ou communiqués dans le cadre des activités commerciales d'entreprises fédérales, et aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales. La *LPRPDÉ* est une loi générale qui s'applique à la collecte des renseignements personnels, peu importe la technologie utilisée. La *LPRPDÉ* s'applique partout au Canada, sauf en Colombie-Britannique, en Alberta et au Québec, où des lois essentiellement similaires régissent le secteur privé, et en Ontario, dans le cas de certaines questions régies par la *Loi sur la protection des renseignements personnels sur la santé*[41].

La *LPRPDÉ* s'applique aussi aux renseignements personnels sur les employés d'une organisation, quand ces renseignements sont recueillis, utilisés ou communiqués dans le cadre des activités d'une *entreprise fédérale*[42]. Divers types d'organisations peuvent être visés par cette loi. Dans la *LPRPDÉ*, la définition d'« entreprise fédérale » inclut expressément les employés des banques, des transporteurs aériens, des chemins de fer, traversiers et compagnies de transport par bateau reliant une province à une autre, et des stations de radiodiffusion. D'autres organismes seront aussi visés par la définition. Par exemple, la commissaire a déjà publié ses observations concernant un fournisseur de services Internet et une centrale nucléaire.

Un ensemble disparate de mesures législatives protègent les renseignements portant sur les employés au Canada. De façon générale, les renseignements personnels sur les employés d'organismes du secteur privé ne sont pas visés par la *LPRPDÉ*, mais les provinces de l'Alberta, de la Colombie-Britannique et du Québec disposent d'une législation sur la protection de la vie privée qui régit les renseignements personnels sur les employés. En outre, les employés des gouvernements provinciaux peuvent être visés par les lois provinciales sur la protection de la vie privée dans le secteur public, lois qui peuvent aussi s'appliquer aux employés des institutions publiques comme les universités et les hôpitaux.

Lorsqu'il appert que les dispositions de la *LPRPDÉ* ou de la *Loi sur la protection des renseignements personnels* s'appliquent, on doit répondre à une autre question. Afin d'être protégés en vertu de ces lois, les renseignements recueillis, utilisés ou communiqués à l'aide de la technologie d'IRF doivent correspondre à la définition de « renseignements personnels » comprise dans ces lois.

3. L'IRF et les renseignements personnels

Aux termes de la *LPRPDÉ*, un « renseignement personnel » constitue « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail[43] ». Si l'on a déterminé que les renseignements sur un employé sont visés par la *LPRPDÉ*, on doit, pour appliquer la Loi, déterminer si les renseignements recueillis, utilisés ou communiqués à l'aide d'un dispositif d'IRF sont des renseignements personnels.

Aux termes de la *Loi sur la protection des renseignements personnels*, les « renseignements personnels » sont définis comme « les renseignements, quels que soient leurs formes et leurs supports, concernant un individu identifiable[44] ». On trouve dans la Loi une liste détaillée d'exemples de renseignements considérés comme des « renseignements personnels », ainsi que quelques exceptions. Les tribunaux ont interprété le terme « renseignements personnels » dans son sens large[45].

Il existe donc plusieurs cas dans lesquels les données contenues dans une étiquette d'IRF constituent des renseignements personnels.

3.1 Renseignements personnels enregistrés sur une étiquette

Dès lors que la micropuce intégrée à l'étiquette d'IRF contient les renseignements personnels d'une personne, elle devient « un entrepôt » de renseignements personnels. Elle pourrait contenir, par exemple, le nom et l'adresse d'une personne, un identifiant clairement associé à une personne, ou encore des données biométriques comme des empreintes digitales numérisées.

3.2 Une étiquette peut devenir un « identificateur » d'une personne

Puisqu'une étiquette d'IRF est unique et que des liens peuvent être établis entre celle-ci et une personne, l'étiquette peut devenir un « identificateur » unique de cette personne. Dans de telles circonstances, elle devient un renseignement personnel. Ce serait également le cas des dispositifs d'IRF intégrés à un insigne ou à un uniforme. Si la lecture d'une étiquette associée à une certaine personne permet d'obtenir des données sur les lieux qu'elle fréquente, il s'agit également de renseignements personnels. Il existe plusieurs cas où l'association de certains renseignements à une personne en particulier forme des renseignements personnels.

Dans la conclusion en vertu de la *LPRPDÉ* nº 319, la commissaire adjointe à la protection de la vie privée a constaté qu'une adresse IP peut être considérée comme un renseignement personnel si des liens peuvent être établis entre celle-ci et une personne identifiable, mais qu'une adresse de port ne constitue pas un renseignement personnel, puisqu'aucun lien ne peut être établi entre celle-ci et une personne identifiable[46]. Suivant cette logique, la commissaire adjointe considérerait que les données inscrites sur une étiquette d'IRF sont des renseignements personnels s'il est possible d'établir des liens entre ces données et une personne en particulier.

Dans la conclusion en vertu de la *LPRPDÉ* nº 270, la commissaire adjointe à la protection de la vie privée a constaté qu'il n'est pas nécessaire que le nom d'une personne soit associé à des renseignements pour que ceux-ci constituent ses renseignements personnels. Si le contexte permet d'identifier la personne, les renseignements en question seront considérés comme des renseignements personnels en vertu de la *LPRPDÉ*[47].

De même, dans une décision rendue en vertu de la *Personal Information Protection Act* (*PIPA*) de l'Alberta, l'enquêteur a indiqué ce qui suit concernant les renseignements captés par surveillance vidéo : « Lorsqu'une caméra de surveillance est allumée, elle recueille des renseignements. Si une personne se trouvant dans son champ de vision peut être identifiée, ces images constituent des "renseignements sur une personne identifiable" [traduction][48] ». Dans un autre rapport d'enquête, l'enquêteur de l'OIPC de l'Alberta s'est penché sur un enjeu semblable à celui-là. Dans ce cas, les renseignements recueillis par l'enregistreur de données de conduite de la voiture concernant des événements qui ont mené à un accident de la route ont été considérés comme étant les

renseignements personnels du conducteur, puisque les renseignements recherchés ont été assimilés à des renseignements sur un conducteur dont l'identité était connue. L'enquêteur a fait remarquer ce qui suit : « On cherchait à obtenir des renseignements détaillés sur la conduite d'E.P. avant l'accident. En conséquence, je suis convaincu que les données recueillies par l'enregistreur de données de conduite constituent des "renseignements sur une personne identifiable" en vertu de la *PIPA* [traduction][49] ».

3.3. Le traitement de renseignements sur des biens peut permettre d'établir un profil

Lorsque des renseignements peuvent être manipulés ou traités et permettent d'établir un profil, il s'agit de renseignements personnels. Il peut s'agir de données recueillies sur les nombreux accès d'une personne à une installation ou au bureau d'un organisme, ou par l'accès à une base de données enregistrant les activités de certaines puces intégrées à des biens manipulés par une personne. Par exemple, en 2006, PricewaterhouseCoopers a annoncé que l'entreprise utiliserait désormais un « système de localisation en temps réel » fondé sur l'IRF à son bureau de Mexico pour connaître les moments auxquels des ordinateurs portatifs et d'autres articles portatifs sortent d'une zone donnée. La base de données enregistrera l'emplacement de l'article et le nom de la personne qui l'a déplacé, et déterminera si le déplacement est autorisé. Lorsque le déplacement n'est pas autorisé, une alarme se déclenchera[50]. Tous ces renseignements permettraient d'établir le profil des activités d'une personne.

3.4 Zones grises

Le contexte du milieu de travail présente quelques problèmes. Dans certains cas, l'information concerne à la fois l'employé à proprement parler et le travail qu'il effectue. Si la caractéristique prédominante de l'information concerne davantage l'emploi que l'employé, l'information constitue un renseignement produit dans le cadre du travail et n'est pas considérée comme un renseignement personnel. Par exemple, dans la conclusion en vertu de la *LPRPDÉ* nº 14, le commissaire à la protection de la vie privée a déterminé que les habitudes de prescription d'un médecin ne correspondaient pas à la définition de renseignements personnels. Le Commissariat n'encourage surtout pas les organisations à appliquer ce raisonnement à plus grande échelle.

Il convient de faire remarquer que la commissaire adjointe à la protection de la vie privée n'a rien relevé dans la *LPRPDÉ* qui indiquerait que les renseignements concernant le travail et les renseignements personnels sont mutuellement exclusifs. Dans la conclusion en vertu de la *LPRPDÉ* nº 220, la commissaire adjointe à la vie privée a maintenu que les relevés de vente attribués à une plaignante afin de comparer son rendement au travail avec celui de ses collègues constituaient des renseignements personnels au sens de la Loi[51]. Comme Scassa et ses collaborateurs l'ont avancé : « Par analogie, une entreprise peut estimer que les renseignements sur les stocks inscrits sur une étiquette d'IRF constituent des renseignements recueillis à des fins commerciales, mais ces renseignements peuvent également constituer des renseignements personnels si des liens peuvent être établis entre ceux-ci et une personne identifiable [traduction][52] ».

L'approche du Commissariat, telle qu'établie dans la présentation au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, consiste à se pencher sur « *la façon dont les renseignements sont utilisés et non sur leur provenance*[53] ».

L'affaire *Dagg c. Canada*[54] illustre également la difficulté de déterminer la catégorie à laquelle se rattachent certains renseignements. Dans cette affaire, en vertu d'une demande d'accès aux renseignements, les employés devaient signer un registre pour accéder à un immeuble pendant les fins de semaine. Le ministère concerné a transmis une partie des renseignements, non pas la totalité, en affirmant que l'information relative aux allées et venues de personnes identifiables constituait des renseignements personnels. La Cour a conclu que l'information demandée avait trait non pas à la personne proprement dite, mais plutôt au poste qu'elle occupe. Même si la Cour a reconnu que la protection des renseignements personnels était en jeu, elle a estimé que ces renseignements concernaient les responsabilités de fonctionnaires. La Cour a jugé la relation aux fonctions publiques suffisante pour déterminer que le droit d'accès avait préséance sur le droit à la vie privée.

Ces cas illustrent les difficultés relatives au traitement des renseignements « hybrides » — renseignements qui ont un caractère personnel mais qui concernent aussi d'autres aspects. Dans l'affaire Dagg, l'enjeu consistait à déterminer si des renseignements particuliers constituaient des renseignements personnels ou des renseignements sur les activités de fonctionnaires. Dans le résumé de la conclusion n° 14, l'enjeu consistait à déterminer si les renseignements en question étaient des renseignements personnels ou des renseignements produits dans le cadre du travail. Le problème de renseignements « hybrides » se pose dans le contexte de la surveillance des employés au travail, puisque la surveillance vidéo, l'écoute de conversations ou l'enregistrement des touches frappées sur le clavier pourraient ne pas être visés par la *LPRPDÉ* s'il est établi que les relevés de la surveillance représentent des renseignements produits dans le cadre du travail.

Même lorsque certaines lois sur la protection des renseignements personnels contiennent une définition des « renseignements sur le produit du travail », comme c'est le cas en Colombie-Britannique[55], il peut être difficile de déterminer quels renseignements constituent des renseignements produits dans le cadre du travail.

Toutefois, il appert clairement, à la lumière de nos conclusions et d'un certain nombre de cas d'arbitrage de conflits de travail[56], que les renseignements recueillis sur un employé par le truchement de techniques de surveillance au travail sont considérés comme des renseignements personnels et que les normes sur la protection de la vie privée s'appliquent.

Nous recommandons aux employeurs d'être extrêmement prudents lorsqu'ils s'appuient sur le concept vaguement défini de « produit du travail » pour contourner les principes relatifs à l'équité dans le traitement de l'information en matière de systèmes de surveillance en milieu de travail comme ceux mettant en cause la technologie de l'IRF.

4. Attente raisonnable en matière de protection de la vie privée en milieu de travail

L'article 3 de la *LPRPDÉ* indique que la Loi a pour objet de fixer des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Le

paragraphe 5(3) confirme le fait que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Le concept de « personne raisonnable » et de ses attentes joue donc un rôle important lorsque vient le moment de tracer la ligne entre les pratiques légitimes et les pratiques portant atteinte à la vie privée en milieu de travail. Si l'organisme recueille, utilise ou communique des renseignements concernant ses employés d'une façon qu'une personne raisonnable considérerait inappropriée dans les circonstances, il viole les normes établies dans la Loi. En conséquence, il convient d'abord de déterminer si la collecte, l'utilisation ou la communication de renseignements personnels est raisonnable.

Les employeurs ont des raisons légitimes de recueillir des renseignements personnels sur leurs employés. Ils ont besoin de savoir qui est la personne qu'ils embauchent. Ils veulent assurer le rendement de leur entreprise et la sécurité physique des lieux de travail. L'employeur peut considérer que la surveillance électronique et toute autre pratique de surveillance sont des moyens nécessaires pour assurer la productivité, éviter toute fuite de renseignements confidentiels et prévenir le harcèlement en milieu de travail[57].

Toutefois, même si l'employeur a un but légitime, cela ne signifie pas que les méthodes qu'il emploie sont raisonnables dans les circonstances. La possibilité qu'un employé puisse commettre un acte préjudiciable ne justifie pas que l'on traite tous les employés comme des suspects. Les avantages discutables qu'il y a à savoir ce que chaque employé fait en tout temps pendant ses heures de travail et avec l'équipement de l'entreprise doivent être évalués en fonction des coûts. Il faut notamment prendre en considération la répercussion de la surveillance sur le moral et la confiance des employés[58]. Il existe une pléiade d'arrêts jurisprudentiels sur des cas d'arbitrage de conflits de travail qui indiquent qu'une surveillance absolue des lieux de travail n'est pas raisonnable[59].

L'atteinte à la vie privée doit également être mesurée en fonction des avantages liés à la collecte de données, et le but de cette mesure doit être fondé sur un besoin pertinent. Pour déterminer si le recours à l'IRF à des fins de surveillance des employés est approprié, il convient de tenir compte du critère en quatre parties suivant, appliqué par la Cour fédérale dans l'affaire *Eastmond c. Chemin de fer Canadien Pacifique*[60].

- La mesure est-elle manifestement nécessaire pour répondre à un besoin particulier?
- Est-il probable qu'elle répondra efficacement à ce besoin?
- L'atteinte à la vie privée est-elle proportionnelle à l'avantage obtenu?
- Existe-t-il un moyen qui porte moins atteinte à la vie privée et permette d'arriver au même but?

Dans la conclusion en vertu de la *LPRPDÉ* n° 279, la commissaire adjointe a constaté que l'utilisation de la surveillance vidéo pour évaluer le rendement d'un employé contrevenait au paragraphe 5(3) de la Loi. Le résumé de cette conclusion contient certaines observations générales concernant l'utilisation de la surveillance vidéo dans le but d'évaluer le rendement d'un employé, qui éclairent les commentaires de la commissaire adjointe sur le contrôle du rendement par l'entremise de la technologie d'IRF :

> *La Loi exige* […] *que le coût de la dignité humaine fasse partie intégrante de l'équation. La surveillance continuelle et sans discrimination des employés* […] *traduit un manque de confiance et fait peser le soupçon sur tous les employés alors que les problèmes peuvent être attribuables à quelques personnes ou à un mode de gestion éventuellement contestable. Elle estime que ce genre de mise en observation omniprésente peut entraver les comportements indésirables mais qu'il contraint également les employés à s'interroger sur la moindre de leurs décisions et le moindre de leurs commentaires. Le respect de la vision de l'entreprise finit par coûter trop cher en termes d'autonomie et de liberté individuelles.*[61]

Dans la conclusion n° 281[62], la commissaire adjointe s'est demandé si l'atteinte à la vie privée découlant de la collecte et de l'utilisation d'une empreinte vocale biométrique était proportionnelle aux avantages que l'entreprise était susceptible d'obtenir. Elle a déterminé que l'utilisation d'une empreinte vocale uniquement à des fins d'authentification personnalisée par un système de mots de passe vocaux ne semblait pas indûment envahissant. L'objectif de ce système avait été expliqué aux employés, et la commissaire adjointe estimait qu'un autre système d'identification ne fournirait pas le niveau de sécurité désiré et ne respecterait donc pas les fins prévues. La partie plaignante a interjeté appel de la décision, mais la Cour fédérale a tranché en sa défaveur[63]. La Cour d'appel fédérale a récemment confirmé la décision de la Cour fédérale. Elle a reconnu qu'une personne raisonnable trouverait justifiées la collecte et l'utilisation d'empreintes vocales biométriques dans un système de mots de passe vocaux, dans les circonstances[64].

4.1. L'implant d'une puce d'IRF est-il raisonnable?

Certaines personnes pourraient soutenir qu'il existe certains métiers pour lesquels les implants électroniques seraient raisonnables, utilisés à des fins limitées, notamment pour localiser un soldat ou un pompier qu'on doit secourir dans une situation d'urgence. Elles pourraient également mentionner les situations exigeant un niveau élevé de sécurité. Par exemple, une entreprise de Cincinnati a récemment implanté des puces dans l'avant-bras de deux employés afin d'assurer un accès sécuritaire restreint à des voûtes contenant des données de nature très délicate[65]. Mais est-il nécessairement plus avantageux d'avoir recours à des étiquettes d'IRF implantées plutôt qu'à ces mêmes étiquettes intégrées à des uniformes, insignes, bracelets ou chevillières? Si le but de l'opération est de cacher le dispositif d'IRF à des fins de sécurité, il faut reconnaître que l'agresseur, tout comme le secouriste, peut posséder un lecteur permettant de repérer la personne recherchée grâce à la puce implantée dans cette dernière. De plus, après les heures de travail, les employés ne pourraient pas enlever la puce implantée.

Implanter une étiquette d'IRF à des employés contre leur volonté est inacceptable en toute circonstance. Une telle pratique suscite des préoccupations en ce qui a trait aux droits fondamentaux de la personne, y compris celui de l'intégrité physique. Aucun critère d'emploi ne devrait être fondé sur la décision d'une personne de se laisser implanter une puce étiquette d'IRF. En effet, il serait pertinent d'envisager des mesures législatives qui interdiraient formellement l'utilisation d'implants d'IRF sous-cutanés sauf dans des situations exceptionnelles.

5. Règles de pratique concernant l'utilisation de l'IRF en milieu de travail

La présente section énumère les mesures que les organismes devraient adopter et les questions qu'ils devraient se poser avant de lancer des applications d'IRF en milieu de travail. Dans certaines

circonstances, les employeurs pourraient conclure, avec raison, que les coûts de certaines applications vont au-delà des avantages potentiels.

L'annexe I de la *LPRPDÉ* contient les principes relatifs à l'équité dans le traitement de l'information. Comme nous l'avons mentionné plus tôt, le Conseil du Trésor a intégré les principes relatifs à l'équité dans le traitement de l'information fondés sur la *LPRPDÉ* au processus d'Évaluation des facteurs relatifs à la vie privée[66] que doivent respecter les établissements fédéraux assujettis à la *Loi sur la protection des renseignements personnels*, et nous avons suivi une approche semblable en ayant recours aux critères fondés sur la *LPRPDÉ*.

Il conviendrait que les organismes vérifient tout d'abord le libellé précis de ces principes[67] pour s'assurer qu'ils respectent la *LPRPDÉ*. Par la suite, il leur faudrait s'inspirer des conseils plus ciblés mentionnés ci-dessous concernant l'application d'IRF qu'ils envisagent. Une série de questions de consultation suit la présente section.

5.1 Reddition de comptes (principe 4.1)[68]

Une personne au sein de l'organisme doit être responsable de l'utilisation du système d'IRF. Les employés doivent facilement savoir qui est cette personne afin de lui poser des questions, au besoin.

La personne responsable du respect de la vie privée doit participer à la conception de tout système d'IRF et doit effectuer une Évaluation des facteurs relatifs à la vie privée[69] (ÉFVP) touchant l'application envisagée avant le déploiement de cette dernière. En abordant les questions touchant la protection de la vie privée dès la conception d'un projet, les organismes peuvent s'assurer que leurs activités liées à l'IRF respectent les lois canadiennes sur la protection de la vie privée et les attentes raisonnables des employés en la matière.

La personne responsable doit être au courant de toute collecte de renseignements personnels par le système d'IRF, de toute utilisation et communication subséquentes ainsi que de la période de conservation de ces renseignements. Elle peut devoir, entre autres, mettre en œuvre des procédures d'approbation d'utilisations nouvelles et non prévues de renseignements recueillis par le système d'IRF et effectuer des ÉFVP. Elle peut également devoir préparer des procédures portant sur l'utilisation non autorisée des registres de contrôle de l'accès.

Toute donnée provenant d'un système d'IRF qui est transférée à une tierce partie à des fins de traitement doit être protégée en vertu d'un contrat qui prévoit une protection comparable au cours du traitement.

Les composantes d'un système d'IRF doivent être étiquetées ou codées et préciser l'identité de l'organisme qui en est responsable. Si on ne connaît pas le dispositif qui recueille les données, il est difficile de respecter les principes de transparence et de reddition de comptes[70].

5.2. Détermination des objectifs (principe 4.2)

Les organismes peuvent établir un équilibre entre leur « besoin de savoir » et le droit de leurs employés à la vie privée s'ils s'assurent de recueillir, d'utiliser et de communiquer des renseignements personnels sur leurs employés uniquement à des fins appropriées.

Le principe de « détermination des objectifs » exige des organismes qu'ils exposent les raisons pour lesquelles les renseignements personnels sont recueillis au moment où l'information est recueillie ou avant qu'elle ne le soit. Dans un contexte d'emploi, l'employeur peut présenter ces diverses raisons dans des manuels destinés à l'employé, des énoncés de politique ou d'autres documents, dans la mesure où ils sont accessibles aux employés. Il est encore plus important, toutefois, que toutes les composantes d'un système d'IRF soient reconnues et marquées afin que leur utilisation soit manifestement claire et transparente.

Il faut informer les employés des raisons pour lesquelles des renseignements personnels sont recueillis par le moyen de la technologie d'IRF. Il convient en outre de détailler et de préciser le plus possible les motifs de l'utilisation, de la collecte et de la communication de renseignements recueillis grâce aux étiquettes d'IRF.

On pourrait façonner la technologie d'IRF de manière à aborder la question de la détermination des objectifs. En effet, l'intégration aux technologies des principes relatifs à l'équité dans le traitement de l'information n'est pas une idée nouvelle. À l'heure actuelle, on s'efforce d'intégrer les pratiques relatives à l'équité dans le traitement de l'information dans les communications entre les lecteurs d'IRF et les étiquettes. Par exemple, Floerkemeier et ses collaborateurs ont démontré comment des « déclarations » visant des objectifs différents pouvaient être utilisées par des lecteurs pour des interrogations différentes, afin d'établir la raison précise pour laquelle une étiquette est lue. Ils ont signalé 14 objectifs précis, notamment « le contrôle d'accès » (les étiquettes d'identification sont lues aux fins du contrôle d'accès, p. ex. en identifiant le titulaire du laissez-passer ou en autorisant l'utilisation d'une clé d'accès), « les mesures contre le vol », « la gestion des actifs » (les étiquettes sont lues pour pouvoir localiser les actifs) et « les services d'urgence » (le système contrôle les étiquettes pour pouvoir offrir aux sauveteurs des renseignements sur l'occupation des locaux)[71].

Peu importe les moyens utilisés, tous les motifs de collecte de renseignements personnels doivent être établis. La collecte de renseignements sur l'emplacement d'un article dans le but de contrôler ses mouvements pourrait permettre de suivre les déplacements d'une personne grâce aux liens établis avec l'identificateur unique de l'étiquette d'IRF. Par exemple, en suivant les déplacements d'une pièce d'équipement dans un lieu du travail, l'employeur peut, de façon indirecte, connaître les activités et les allées et venues des employés autorisés à utiliser cet équipement. Si l'objectif du suivi peut être jugé raisonnable, il faut cependant cerner séparément le but de la collecte de renseignements personnels (voir « Collecte limitée »)[72].

5.3. Consentement (principe 4.3)

Les principes relatifs à l'équité dans le traitement de l'information reposent sur le consentement. Si un organisme désire recueillir des renseignements personnels par le moyen de la technologie d'IRF, il doit également, après avoir informé les employés de l'objet de la collecte de renseignements, obtenir leur consentement.

Selon le principe 4.3.2, un employé doit être informé de toute collecte, utilisation ou communication de renseignements personnels et y consentir. Dans la conclusion en vertu de la *LPRPDÉ* nº 273[73], la commissaire adjointe a constaté que l'organisation visée n'avait pas fait d'efforts raisonnables pour informer ses employés de la surveillance vidéo limitée dont ils faisaient l'objet (surveillance que la commissaire adjointe estime raisonnable dans la situation). L'employeur avait affiché une note de service pour informer les employés de la façon dont seraient utilisés les renseignements recueillis par

les caméras, mais les employés n'étaient pas au courant de la note de service en question. Pour régler la plainte, la commissaire adjointe a recommandé que l'organisation élabore et rende accessible un document de politique expliquant l'utilisation faite de la surveillance par caméra, pour respecter les prescriptions du principe 4.1.4.

Puisque les systèmes d'IRF sont un phénomène relativement nouveau (ou qui passe peut-être inaperçu) en milieu de travail, de nombreux employés ne connaissent pas bien la technologie, son fonctionnement et la façon dont les données sont recueillies, utilisées et stockées. Les organismes qui mettent en place un système d'IRF ne devraient pas se contenter de diffuser des documents à ce sujet; ils devraient renseigner les employés au sujet de ce système.

Les organismes devraient prendre note du fait que, dans l'affaire *Englander c. Telus Communications Inc*[74], la Cour d'appel fédérale a confirmé qu'un organisme doit s'efforcer d'aider les personnes à comprendre leur droit à la vie privée. La Cour a déterminé qu'il incombe aux organismes d'informer les personnes des buts principaux et secondaires qui motivent la collecte, l'utilisation et la communication de tout renseignement personnel, ainsi que des options qui s'offrent à ces personnes dans des cas particuliers, y compris la possibilité de se retirer d'un projet précis de collecte, d'utilisation ou de communication de renseignements personnels. La question en litige dans l'affaire Englander concernait la décision d'un client d'une compagnie de téléphone cellulaire d'accepter que son nom, son adresse et son numéro de téléphone figurent dans un annuaire téléphonique. La Cour a déterminé que la société Telus avait violé la *LPRPDÉ* parce qu'elle n'avait pas déployé d'efforts raisonnables pour s'assurer que ses clients étaient informés des fins auxquelles les renseignements personnels seraient utilisés et que la compagnie n'avait pas informé de façon adéquate ses clients de la possibilité de ne pas faire inscrire leurs renseignements dans l'annuaire téléphonique public.

En vertu de la *LPRPDÉ*, le consentement doit être libre et éclairé. Mais une question se pose souvent dans le cadre de la *LPRPDÉ* : peut-on considérer que le consentement d'un employé est véritablement volontaire lorsque son employeur exige de lui, à titre de condition d'emploi, qu'il consente à la collecte et à l'utilisation de ses renseignements personnels en milieu de travail? Il arrive que des employeurs prennent la décision de mettre en place des caméras de surveillance vidéo, des systèmes GPS et des systèmes de sécurité biométriques; cela reflète une tendance de plus en plus importante à l'augmentation de la surveillance au travail pour de nombreuses raisons, y compris la sécurité, la sécurité des produits, la gestion du rendement ou l'efficience de l'entreprise[75]. La technologie d'IRF ajoute une autre dimension à la surveillance en milieu de travail. Il ne faut pas oublier que l'on doit recueillir, utiliser ou communiquer des renseignements personnels uniquement à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. Un employé ne peut certainement pas être tenu, en raison de conditions d'emploi, de consentir à une pratique de collecte de renseignements qui ne respecterait pas ce critère.

L'article 7 de la *LPRPDÉ* prévoit plusieurs situations dans lesquelles les renseignements personnels peuvent être recueillis, utilisés ou communiqués sans le consentement de la personne visée, notamment « à des fins liées à une enquête sur la violation d'un accord ou la contravention de droit fédéral ou provincial » ou lorsque le « consentement de l'intéressé [peut] compromettre l'exactitude du renseignement[76] ». Dans l'affaire *Eastmond c. Chemins de fer Canadien Pacifique*, la Cour fédérale s'est dite d'avis que cette exception s'applique à la surveillance vidéo en milieu de travail visant à déceler les cas de vol[77]. Des exceptions à l'exigence d'obtenir le consentement s'appliquent également à la collecte de renseignements, par un organisme, visant à communiquer de son propre chef au gouvernement des enjeux touchant la sécurité nationale, la défense du Canada ou la conduite d'affaires internationales. Ces exceptions pourraient s'avérer importantes dans le cadre de la

technologie d'IRF, puisque l'IRF donne aux organismes la possibilité de recueillir une quantité sans précédent de renseignements personnels. Il faudrait mettre au courant les employeurs, les employés et les syndicats des questions découlant de ces dispositions de la Loi.

5.4. Collecte limitée (principe 4.4)

Le principe de collecte limitée précise que les renseignements ne peuvent être recueillis de façon arbitraire; la collecte doit se limiter à ce qui est nécessaire dans le contexte de l'emploi. Il est souvent difficile pour un employé de déterminer si un organisme respecte cette pratique parce que, dans la plupart des cas, l'employé ne peut réellement savoir si la collecte de données se fait de façon non conforme ou si les fins de la collecte ne sont pas celles qui ont été déterminées.

Les organismes doivent s'assurer que toute collecte de données est directement liée aux fins raisonnables et légitimes auxquelles l'employé a consenti.

5.4.1. Limites de la collecte sur le plan technologique

Pour limiter la collecte de renseignements, on pourrait, entre autres, mettre en place des mécanismes qui brouillent la transmission par des étiquettes non ciblées. Tout particulièrement, au lieu d'envoyer des signaux arbitraires et de filtrer par la suite les étiquettes d'intérêt dans le but de les conserver, les demandes de lecture pourraient viser uniquement les étiquettes pertinentes[78]. La deuxième option est de supprimer immédiatement les données recueillies qu'il n'était pas nécessaire de recueillir en premier lieu.

Les organismes pourraient configurer la technologie de façon à tenir compte de pratiques de collecte distinctes. Par exemple, Floerkemeier et ses collaborateurs ont cerné quatre de ces pratiques :

- Surveillance anonyme : Ce procédé permet de recueillir l'information sans avoir à connaître le numéro d'identification unique d'une étiquette. Floerkemeier donne en exemple les applications des capteurs permettant d'ouvrir des portes automatiques ou de dénombrer des articles dans un secteur donné[79].

- Identification locale : Ce procédé permet de déterminer la présence de certains articles dans un secteur donné, mais n'indiquera pas d'où ils proviennent. La divulgation des emplacements antérieurs d'un article serait interdite à moins d'une raison valable convaincante comme une enquête criminelle. Une déclaration d'utilisation qui ne concerne que l'identification locale garantirait à l'employé que ses déplacements ne font pas l'objet d'une surveillance.

- Repérage d'articles : Cette pratique est plus exhaustive que l'identification locale et permet de suivre les déplacements des articles. Ce procédé permettrait aussi de suivre les allées et venues d'un employé grâce à l'établissement de liens entre l'employé et le numéro d'identification unique de l'étiquette d'IRF.

- Repérage de personnes : un système pour le milieu de travail pourrait être conçu de façon à recueillir des renseignements sur les allées et venues d'un employé. Pour ce faire, l'organisme pourrait, par exemple, utiliser des étiquettes d'IRF

intégrées dans des cartes d'identification ou des uniformes. Il est également possible de recueillir de tels renseignements par le truchement d'un système de repérage d'articles, si des liens peuvent être établis entre l'article en question et une personne identifiable. Si le système de repérage d'articles est également utilisé pour le repérage de personnes, il est nécessaire de faire état de cet autre objectif de la collecte de renseignements[80]. Le repérage de personnes soulèvera sans soute davantage d'enjeux relatifs à la protection de la vie privée que le repérage d'articles.

Il serait possible d'utiliser ces déclarations relatives à la collecte pour conserver à certaines étiquettes un caractère anonyme, lorsque c'est possible[81]. En gardant cet aspect à l'esprit, les organismes devraient tenir compte du critère en quatre points que le Commissariat a utilisé au moment d'évaluer le caractère raisonnable de la collecte de données (voir section 4).

Lorsque c'est possible, il est préférable d'assurer une surveillance anonyme au lieu d'un contrôle qui permettrait d'identifier l'employé. Les réponses anonymes font déjà partie de certains protocoles d'IRF.

Floerkemeier et ses collaborateurs indiquent également qu'on pourrait utiliser une version perfectionnée d'une étiquette d'IRF ordinaire, une sorte d'« étiquette chien de garde », pour assurer une certaine transparence dans le cadre d'un processus de détection d'étiquette par ailleurs invisible. Ce type d'étiquette pourrait être utilisé conjointement avec les autres caractéristiques intégrées relatives à la protection de la vie privée dont on a déjà discuté. L'étiquette permettrait de décoder les commandes envoyées par le lecteur et les afficherait sur un écran à des fins d'inspection. Ce type d'étiquette « chien de garde » pourrait enregistrer tous les transferts de données afin que les employés puissent y accéder sur demande. La puce chien de garde pourrait être un dispositif discret, ou encore ses fonctions pourraient être intégrées à un téléphone cellulaire[82]. L'étiquette chien de garde pourrait renforcer la transparence en permettant de connaître l'identification de l'opérateur, le but de la collecte, le type de données recueillies et le type d'étiquettes ciblées.

5.5. Utilisation, communication et conservation limitées (principe 4.5)

Les organismes ne doivent pas utiliser ni communiquer des renseignements personnels à des fins autres que celles auxquelles ces derniers ont été recueillis, à moins que la personne concernée y consente ou que la loi ne l'exige. Lorsque l'organisme dispose déjà de renseignements et qu'il souhaite les utiliser ou les communiquer à de nouvelles fins, le consentement de l'employé est requis. Par exemple, si un employeur a recueilli des renseignements grâce à l'IRF pour suivre un équipement et qu'il établit des liens entre ces renseignements et les renseignements personnels de l'employé à des fins disciplinaires, il outrepasserait la portée de la collecte initiale.

Les organismes devraient éviter l'utilisation de systèmes d'IRF dans le but de recueillir des renseignements dans le cadre de mesures disciplinaires avant de passer la situation au crible du critère de la personne raisonnable en quatre parties.

Les renseignements qui ont été recueillis par inadvertance devraient être immédiatement supprimés de façon sécuritaire. Les organismes ne doivent conserver les renseignements personnels qu'aussi longtemps qu'ils en ont besoin pour réaliser les fins auxquelles l'information a été recueillie. Lorsque l'information n'est plus nécessaire, on doit la supprimer immédiatement, de façon sécuritaire, en tenant compte des exigences relatives aux droits d'accès de l'employé.

5.6. Exactitude (principe 4.6)

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.

Les organismes peuvent faire face à un cas où un employé conteste l'exactitude des renseignements recueillis par le système d'IRF. Par exemple, un employé peut contester l'enregistrement d'un lecteur qui, selon lui, n'a pas eu lieu[83]. Il est possible que d'autres personnes utilisent l'uniforme, l'insigne ou d'autres articles munis d'une étiquette d'IRF contenant des renseignements appartenant à un employé, avec ou sans son consentement. De plus, le piratage ou l'altération de données constituera un important problème pour les organismes, les syndicats et les employés. Par exemple, l'insigne muni d'un dispositif d'IRF d'un employé travaillant dans un aéroport ou une installation nucléaire peut être une cible de choix pour une personne non autorisée qui cherche à accéder à un lieu sécurisé.

Les fournisseurs doivent produire, à l'intention des organismes et des employés, une analyse du risque lié à l'exactitude des renseignements fournis par leurs systèmes d'IRF, selon les applications en question. Grâce à cette information, les organismes et les employés connaîtront les limites perçues d'un système d'IRF en particulier; ils seront davantage en mesure de savoir quand remettre en question les conclusions tirées des renseignements issus du système en question.

5.7. Protection (principe 4.7)

Les renseignements personnels doivent être protégés à un niveau correspondant à leur degré de sensibilité. La sensibilité des renseignements peut varier selon le contexte. Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol, la communication, la reproduction, l'utilisation, la modification ou l'accès non autorisés (voir « L'IRF et les risques pour la sécurité »). Les renseignements personnels qui ne sont plus nécessaires aux fins déterminées doivent être supprimés de façon sécuritaire.

5.8. Transparence (principe 4.8)

Il est essentiel qu'un organisme qui utilise des systèmes d'IRF consacre assez de temps et de ressources pour informer ses employés du fonctionnement de la technologie, de l'emplacement des étiquettes et des lecteurs d'IRF, du type de renseignements recueillis et de l'utilisation prévue des renseignements. Il faut informer les employés des articles précis qui sont munis d'une étiquette d'IRF et qui se trouvent dans leur environnement (notamment les produits, les emballages, les outils et autres biens) et l'emplacement de tous les lecteurs.

Il faut aussi leur montrer la manière dont les renseignements sont recueillis en milieu du travail. Par exemple, les employés doivent savoir que les étiquettes d'IRF transmettent des renseignements sans que l'employé ne fasse quoi que ce soit.

On doit indiquer aux employés si des liens seront établis entre les renseignements tirés du système d'IRF et d'autres renseignements personnels et si ces derniers seront communiqués à des tiers.

Il ne doit pas y avoir d'étiquettes ou de lecteurs d'IRF dissimulés. Afin d'annoncer le fait qu'une étiquette d'IRF est lue, on peut apposer une affiche près du lecteur ou faire en sorte que le lecteur émette un son ou un voyant lumineux lorsqu'il lit une étiquette. En outre, une étiquette munie d'une mémoire pourrait compter le nombre de fois qu'elle est lue[84].

Il est également important de connaître l'emplacement de l'ensemble des étiquettes et des lecteurs, puisqu'il est possible que les systèmes d'IRF interfèrent avec des dispositifs médicaux actifs implantés. La Commission internationale de protection contre les rayonnements non ionisants s'est penchée sur cette question en 2002, mais on doit mener davantage de recherches à ce sujet pour déterminer si c'est réellement le cas[85].

5.9 Accès individuel (principe 4.9)

Les employés ont le droit d'accéder aux renseignements personnels qui les concernent recueillis par leur employeur. Pour exercer leur droit d'accès, les employés doivent connaître l'ampleur de la collecte qui a lieu. Il ne doit exister aucune étiquette ni aucun lecteur d'IRF caché. Il est difficile, voire impossible, pour un employé de demander des renseignements liés à une étiquette dont il ne connaît pas l'existence, ou de s'informer des données recueillies par un lecteur caché. En conséquence, tous les lecteurs d'IRF doivent être identifiables si l'on veut que les employés puissent demander accès aux renseignements personnels recueillis et déterminer si les données recueillies ont été utilisées à des fins auxquelles ils n'ont pas fourni leur consentement.

Par exemple, si une employée désire obtenir toutes les données qui sont liées à sa carte d'employée munie d'un dispositif d'IRF, elle pourrait demander[86] :

- une copie papier des renseignements inscrits sur sa carte, présentés dans un langage simple;
- tous les dossiers dans lesquels sont consignées ses allées et venues dans un édifice et des installations, y compris l'accès et la facturation en ce qui concerne les stationnements et la cafétéria, s'il s'agit de la même carte;
- tous les relevés de communication de ses données à des tierces parties;
- tous les dossiers et documents techniques qui lui permettraient de comprendre quels types de lecteurs, autres que ceux de l'employeur, pourraient lire sa carte en partie ou en totalité.

Cette employée pourrait aussi vouloir connaître toutes les utilisations qui ont été faites des renseignements recueillis par sa carte, y compris les décisions qui ont été prises la concernant. Par exemple, si l'employeur utilisait les renseignements recueillis par une carte d'IRF pour étayer ses jugements concernant son rendement, l'employée aurait ainsi l'occasion de contester le caractère raisonnable de cette fin et l'exactitude des renseignements recueillis.

5.10 Contestation de la conformité (principe 4.10)

Un employé doit être en mesure de s'opposer au non-respect, par l'organisme, des autres principes en présentant une demande de renseignements ou en déposant une plainte. L'organisme doit étudier chaque plainte qu'il reçoit en temps opportun et fournir une réponse exhaustive à l'employé.

Une personne peut déposer une plainte auprès du Commissariat ou du commissaire provincial compétent si, par exemple, elle estime qu'un organisme a utilisé la technologie d'IRF pour recueillir des renseignements personnels de façon subreptice ou que la collecte de renseignements allait au-delà des fins déterminées. Outre les employés d'entreprises fédérales, les employés d'entreprises privées dans les provinces qui ne disposent pas de mesures législatives visant le secteur privé n'ont pas ce droit.

6. L'IRF en milieu de travail : Conclusion

> *La première chose à faire, c'est de trouver le point d'équilibre entre les droits et les besoins de la société, ou encore entre la commodité et la sécurité, au regard des droits de la personne, naturellement moins attrayants, toujours rebutants et toujours difficiles et qui restent simplement fondamentaux.*[87]
> — John Godfrey, citation tirée du document *La vie privée : où se situe la frontière?*, rapport présenté au Comité permanent des droits de la personne et de la condition des personnes handicapées (1997, p. 15).

En milieu de travail, les bonnes pratiques en matière de protection des renseignements personnels ne se limitent pas à éviter les plaintes, les griefs ou les poursuites judiciaires. Que les droits à la protection des renseignements personnels soient protégés par des dispositions législatives ou par contrat, le fait de favoriser, en milieu de travail, une culture où la protection de la vie privée est jugée importante et respectée contribue au maintien du moral et de la confiance mutuelle, et représente une approche raisonnable[88].

Les enjeux touchant les renseignements personnels découlant de la surveillance en milieu de travail n'est pas un phénomène nouveau, mais la technologie continue de renforcer la capacité des employeurs de surveiller un très large éventail d'activités ayant lieu en milieu de travail. La technologie d'IRF offre un autre outil de surveillance en milieu de travail. Néanmoins, l'IRF pose des problèmes particuliers : comme il s'agit d'une nouvelle technologie encore mal comprise par bon nombre d'entre nous, les personnes qui y ont recours ne connaissent pas bien toutes ses capacités et les avenues qu'elle offre, et l'IRF peut être utilisée de façon diffuse et invisible. Ces caractéristiques exigent que l'on prenne beaucoup de précautions au moment d'intégrer la technologie d'IRF au milieu de travail, pour s'assurer de respecter le droit à la vie privée des employés.

Lorsque les employeurs envisagent de mettre en place de nouvelles technologies en milieu de travail, ils devraient mener une évaluation des facteurs relatifs à la vie privée. De plus, les considérations relatives à la protection des renseignements personnels devraient orienter le choix d'un système en particulier ou influer sur la personnalisation d'une technologie en milieu de travail. Même si les nouvelles technologies ont la capacité de porter atteinte à la vie privée, elles peuvent également être configurées de façon à tenir compte des préoccupations relatives à la protection des renseignements personnels ou à limiter les risques pour la protection de la vie privée et la sécurité. Le présent document anticipe, dans une grande mesure, le déploiement de l'IRF en milieu de travail et, vu sous cet angle, il vise entre autres à inciter les employeurs à tenir compte de la législation relative à la protection de la vie privée au moment de choisir et de mettre en place un système d'IRF.

Même si le choix d'adopter un système d'IRF appartient en grande partie à l'employeur, les employés et les syndicats qui les représentent ont aussi un rôle à jouer dans la protection de leurs renseignements personnels. Lorsque c'est possible, les employés devraient participer au choix et à la

mise en place des systèmes d'IRF en milieu de travail. L'intervention des employés d'entrée de jeu peut permettre d'accroître leur autonomie et leur dignité et favorise aussi l'obtention de leur consentement aux fins visées de la technologie. En outre, il est louable d'éviter autant que possible l'identification de personnes. L'apposition d'étiquettes d'IRF sur des produits et des biens peut être bénéfique pour les organismes et présenter peu de risques envers la protection de la vie privée. Par contre, l'étiquetage des employés par l'entremise de pièces d'identité, d'uniformes, de chevillières et de bracelets soulève nécessairement des questions de vie privée qui pourraient être évitées en utilisant d'autres approches.

Les valeurs d'autonomie et de dignité sont également renforcées par la mise en place d'une technologie respectueuse des employés. Les employeurs qui désirent introduire de nouvelles technologies, notamment l'IRF, en milieu de travail devraient prendre le temps d'informer et de sensibiliser leurs employés concernant la technologie, les exigences particulières de sa mise en place, son fonctionnement et le type de renseignements recueillis. Dans certains cas, les employeurs pourraient conclure, avec raison, que le coût de certaines applications est supérieur aux avantages potentiels de ces dernières.

PARTIE III – Consultation : Questions

Tous les commentaires concernant le présent document sont les bienvenus, afin d'enrichir le débat au sujet des systèmes d'IRF en milieu de travail. Nous souhaitons tout particulièrement obtenir les commentaires des personnes qui seraient éventuellement directement touchées par l'IRF en milieu de travail, c'est-à-dire les employeurs, les employés et les syndicats, de même que les commentaires de développeurs de technologie d'IRF.

Afin d'alimenter le débat, nous soumettons des questions générales auxquelles nous espérons recevoir des réponses.

1. Quand les systèmes d'IRF sont utilisés en milieu de travail, on doit tenir compte de la dignité des personnes et utiliser le critère de la personne raisonnable en quatre parties.
   - Quels paramètres devraient être utilisés?
   - Quels usages des systèmes d'IRF devraient être interdits en milieu de travail?

2. Les systèmes d'IRF devraient être conçus et adaptés en fonction des principes relatifs à l'équité dans le traitement de l'information avant leur déploiement.
   - Comment peut-on encourager les fournisseurs à remplir et à transmettre à leurs clients une Évaluation des facteurs relatifs à la vie privée (ÉFVP) au sujet d'un système d'IRF?
   - Comment les organisations qui envisagent le déploiement d'un système d'IRF peuvent-elles vérifier de manière indépendante les affirmations faites par le fournisseur au sujet de la conformité du système aux principes de protection de la vie privée?
   - Comment peut-on encourager les employeurs à exiger une ÉFVP dûment remplie avant le déploiement d'un système d'IRF, afin de s'assurer que celui-ci a été élaboré de manière à respecter les lois visant la protection de la vie privée?

3. Les systèmes d'IRF devraient être configurés de manière à ne recueillir que le minimum nécessaire afin d'atteindre leurs objectifs.
   - Comment peut-on encourager les employeurs à configurer leurs systèmes d'IRF afin qu'ils effectuent une surveillance anonyme, si possible, de manière à ce que l'information puisse être recueillie sans que l'on connaisse l'identité d'une étiquette particulière?
   - Comment peut-on encourager les employeurs à déterminer la présence d'un article dans un endroit particulier sans lier cette information aux déplacements de cet article d'un endroit à l'autre?

4. Il ne devrait pas y avoir d'étiquettes ou de lecteurs d'IRF dissimulés.
   - Étant donné que l'industrie a tendance à réduire la taille des étiquettes d'IRF (et à rendre les lecteurs plus facilement dissimulables), quelles stratégies pourraient faire en sorte que les systèmes d'IRF soient plus évidents en milieu de travail?

5. Les employeurs devraient consulter leurs employés (et les syndicats) avant d'introduire en milieu de travail des systèmes de surveillance ou des technologies ayant le potentiel de servir à cette fin comme les systèmes d'IRF.
   - Selon vous, y a-t-il des groupes ou des types de travailleurs qui seraient particulièrement vulnérables à la surveillance par système d'IRF?

6. Les employés doivent être avertis si des renseignements tirés d'un système d'IRF seront liés à d'autres renseignements personnels et si ces renseignements seront communiqués à des tiers.
   - Quels couplages de données devraient être interdits?
   - Quels renseignements personnels pourraient être liés à un système d'IRF de manière légitime, et dans quelles circonstances?

7. En toute circonstance, il est inacceptable d'implanter des étiquettes d'IRF aux employés contre leur gré. Accepter l'implantation d'une étiquette d'IRF ne devrait jamais constituer un critère d'embauche.
   - Quels autres critères méritent notre attention dans le cadre du débat sur l'implantation de dispositifs d'IRF en milieu de travail?

8. Quelles stratégies recommanderiez-vous à la communauté des commissaires à la protection de la vie privée pour traiter cet enjeu pendant la prochaine année?

9. Quelles solutions de rechange aux IRF sont disponibles pour éviter les risques d'atteinte à la vie privée présentés dans le présent document?

Nous émettrons nos recommandations finales au sujet des règles de pratique, y compris un rapport sur les commentaires que nous aurons reçus, après la clôture de la période de consultation.

Veuillez faire parvenir par la poste vos commentaires sur le document de consultation sur l'IRF au Commissariat à la protection de la vie privée du Canada avant le 30 avril 2008 :

Consultation sur l'IRF
Commissariat à la protection de la vie privée du Canada
112, rue Kent
Place de Ville
Tour B, 3e étage
Ottawa (Ontario)
K1A 1H3

Nous préférons recevoir vos commentaires par courriel, au :

consultation@privcom.gc.ca

N'hésitez pas à communiquer avec nous pour toute information :

Sans frais : 1-800-282-1376
Téléphone : 613-995-8210
Télécopieur : 613-947-6850
ATS : 613-992-9190

Annexe I — Technologie d'IRF

En général, les étiquettes peuvent être divisées en trois catégories principales : passives, semi-passives et actives. La catégorisation se fait en fonction de la présence ou de l'absence d'une pile, ce qui a une répercussion sur le champ de lecture de l'étiquette. Les étiquettes passives sont les plus simples, puisqu'il n'y a ni source d'énergie ni transmetteur intégré. Pour être activées, elles doivent recevoir un signal transmis par un lecteur. Puisque les étiquettes passives n'ont pas de pile, elles sont beaucoup plus petites et moins chères que les étiquettes actives. Une étiquette passive peut-être lue à une distance maximale de cinq mètres.

Les étiquettes semi-passives ont une pile, mais puisqu'elles n'ont pas de transmetteur intégré, la communication se fait toujours grâce à un lecteur. Leur champ de lecture est néanmoins beaucoup plus important que celui d'une étiquette passive — jusqu'à un maximum de 100 mètres[89].

Les étiquettes actives d'IRF disposent d'une pile et d'un transmetteur actif. Les étiquettes actives sont en général plus grandes que les étiquettes passives et peuvent être lues à une plus grande distance. Leur champ de lecture est également plus important que celui des étiquettes semi-passives, puisque les étiquettes actives sont munies de leur propre transmetteur[90].

Les étiquettes existent en mode lecture seule ou en mode lecture-écriture. Ces termes renvoient à la capacité des puces de modifier ou de supprimer des renseignements. Une étiquette en mode lecture seule est un type d'étiquette d'IRF qui ne sera associé qu'à un seul numéro d'identification, tandis qu'une étiquette en mode lecture-écriture permettra la modification des données entreposées[91]. Des étiquettes d'IRF plus perfectionnées peuvent contenir une mémoire en mode de lecture-écriture qui peut être programmée par un lecteur, et elles peuvent aussi contenir des renseignements biométriques ou même des capteurs qui permettent de déceler les changements de niveau d'humidité ou de pression autour de l'étiquette.

La conception de certaines étiquettes d'IRF permet à ces dernières de communiquer avec tout lecteur (on parle parfois d'étiquettes « volages »). De même, la conception de certaines étiquettes peut limiter la communication à un seul lecteur, duquel elles exigent le code d'authentification avant de transmettre une information (on parle d'étiquettes « sécurisées »).

Un lecteur d'IRF, ou un interrogateur, est un dispositif qui permet de communiquer avec l'étiquette d'IRF. Il émet un signal radio que capte l'étiquette. Celle-ci envoie ensuite de l'information au lecteur. Le lecteur peut prendre la forme d'un dispositif portable à main ou d'un dispositif que l'on fixe dans des endroits stratégiques, comme les quais de chargement pour l'expédition ou la réception de marchandises, sous les moquettes ou dans les entrées de porte.

Pour de plus amples renseignements sur la technologie d'IRF, consultez les ressources énumérées à l'annexe II.

Annexe II – Sources choisies sur l'IRF

Katherine Albrecht et Liz Mcintyre. *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Nashville, Nelson Current, 2005. http://www.spychips.com/.

Edward Balkovich et coll. *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*, RAND Corporation, 2005. http://www.rand.org/pubs/technical_reports/TR197/.

Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario. *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, février 2004. http://www.ipc.on.ca/images/Resources/up-rfid.pdf.

Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario. *Privacy Guidelines for RFID Information Systems*, juin 2006. http://www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf.

Center for Democracy and Technology, *CDT Working Group on RFID: Best Practices for Deployment of RFID Technology*, 1er mai 2006. http://www.cdt.org/privacy/20060501rfid-best-practices.php.

Autorité de protection des données des Pays-Bas. *RFID: Promising or Irresponsible? Contribution to the social debate about RFID*, La Haye, octobre 2006. http://www.dutchdpa.nl/documenten/en_rap_2006_rfid.shtml?refer=true.

Electronic Frontier Foundation. *Radio Frequency Identification (RFID)*. http://www.eff.org/Privacy/RFID/.

Electronic Privacy Information Center, *Radio Frequency Identification (RFID) Systems*. En ligne : EPIC: http://www.epic.org/privacy/rfid/.

Commission européenne, Société de l'information. *Towards an RFID Policy for Europe*. http://ec.europa.eu/information_society/policy/rfid/index_en.htm.

Parlement européen, Évaluation des options technologiques et scientifiques. *RFID and Identity Management in Everyday Life*, IPOL/A/STOA/2006-22. http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

Federal Trade Commission. *RFID Radio Frequency Identification: Applications and Implications for Consumers*, mars 2005. http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

Christian Floerkemeier et coll. *Scanning with a Purpose: Supporting the Fair Information Principles in RFID Protocols*, Institute for Pervasive Computing, Suisse, 2004. http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf. (Également disponible dans Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda et Michiaki Yasumura (dir. publ.). *Ubiquitous Computing Systems : Second International Symposium*, UCS, Tokyo, Japon, 8–9 novembre 2004, documents choisis révisés, Berlin, Springer-Verlag, 2005, p. 214–231.)

Simson Garfinkel et Beth Rosenberg, (dir. publ.). *RFID: Applications, Security, and Privacy*, New Jersey, Pearson Education, 2005.

Conférence internationale des commissaires à la protection des données et de la vie privée. *Résolution sur l'identification par radiofréquence*, 20 novembre, 2003. http://www.privacyconference2003.org/resolutions/res5.DOC.

Union internationale des Télécommunications. *The Internet of Things*, novembre 2005. http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.

Ari Juels. *RFID Security and Privacy: A Research Survey*, RSA Laboratories, 28 septembre 2005. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf#search=%22rfid%20contactless%20card%20distinctions%22.

Gaétan Laberge, Commission d'accès à l'information du Québec. *Radiofrequency identification technology (RFID): is there reason to mistrust it?*, mai 2006. http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf.

Commissariat à la protection de la vie privée du Canada. *Fiche d'information : l'identification par radiofréquence*. http://www.privcom.gc.ca/fs-fi/02_05_d_28_f.asp.

Organisation de coopération et de développement économiques. *Identification par radiofréquence (RFID) : facteurs incitatifs, enjeux et considérations*, 4 avril 2006, p. 8. http://www.olis.oecd.org/olis/2005doc.nsf/809a2d78518a8277c125685d005300b2/86adbbc99efbb1aec12571220053a130/$FILE/JT03206925.PDF.

Teresa Scassa, Theodore Chiasson, Michael Deturbide et Anne Uteck. *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, avril 2005. http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf.

Annexe III – Portée de l'application de la *LPRPDÉ* et de la *Loi sur la protection des renseignements personnels*

***Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*), C.S. 2000, ch. 5.**

La *LPRPDÉ* s'applique aux renseignements personnels des employés qui travaillent dans des « entreprises fédérales ».

« Entreprises fédérales » : les installations, ouvrages, entreprises ou secteurs d'activité qui relèvent de la compétence législative du Parlement. Sont compris parmi les entreprises fédérales :

a) les installations, ouvrages, entreprises ou secteurs d'activité qui se rapportent à la navigation et aux transports par eau, notamment l'exploitation de navires et le transport par navire partout au Canada;

b) les installations ou ouvrages, notamment les chemins de fer, canaux ou liaisons télégraphiques, reliant une province à une autre, ou débordant les limites d'une province, et les entreprises correspondantes;

c) les lignes de transport par bateaux à vapeur ou autres navires, reliant une province à une autre, ou débordant les limites d'une province;

d) les passages par eaux entre deux provinces ou entre une province et un pays étranger;

e) les aéroports, aéronefs ou lignes de transport aérien;

f) les stations de radiodiffusion;

g) les banques;

h) les ouvrages qui, bien qu'entièrement situés dans une province, sont, avant ou après leur réalisation, déclarés par le Parlement être à l'avantage général du Canada ou à l'avantage de plusieurs provinces;

i) les installations, ouvrages, entreprises ou secteurs d'activité ne ressortissant pas au pouvoir législatif exclusif des législatures provinciales;

j) les installations, ouvrages, entreprises ou secteurs d'activité auxquels le droit, au sens de l'alinéa a) de la définition de « droit » à l'article 2 de la *Loi sur les océans*, s'applique en vertu de l'article 20 de cette loi et des règlements pris en vertu de l'alinéa 26(1)k) de la même loi.

***Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21.**

La *Loi sur la protection des renseignements personnels* s'applique aux institutions fédérales. Par « institutions fédérales », la Loi entend :

a) tout ministère ou département d'État relevant du gouvernement du Canada, ou tout organisme, figurant à l'annexe;

b) toute société d'État mère ou filiale à cent pour cent d'une telle société, au sens de l'article 83 de la *Loi sur la gestion des finances publiques*.

Notes

1. L.C. 2000, c. 5. En ligne : ministère de la Justice Canada : http://laws.justice.gc.ca/fr/showtdm/cs/P-8.6.
2. S.R.C., 1985, c. P-21. En ligne : ministère de la Justice Canada : http://laws.justice.gc.ca/fr/showtdm/cs/P-21.
3. L.C. 2000, c. 5. En ligne : ministère de la Justice Canada : http://laws.justice.gc.ca/fr/showtdm/cs/P-8.6.
4. S.R.C., 1985, c. P-21. En ligne : ministère de la Justice Canada : http://laws.justice.gc.ca/fr/showtdm/cs/P-21.
5. Commissaire à la protection de la vie privée du Canada. *Rapport annuel au Parlement 2005, Rapport sur la Loi sur la protection des renseignements personnels et les documents électroniques*. En ligne : Commissariat à la protection de la vie privée, http://www.privcom.gc.ca/information/ar/200506/2005_pipeda_f.asp#020.
6. Valerie Steeves, professeure, devant le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie à propos du projet de loi S-21 qui vise à garantir le droit des personnes à la vie privée, 20 septembre 2001. En ligne : Gouvernement du Canada : http://www.parl.gc.ca/37/1/parlbus/commbus/senate/com-f/soci-f/25ev-f.htm.
7. M. Weiser, « The Computer for the 21st Century », *Scientific American,* vol. 265, n° 3 (1991), p. 94–104.
8. Ari Juels, *RFID Security and Privacy: A Research Survey*, RSA Laboratories, 28 septembre 2005, p. 3. En ligne (en anglais seulement) : http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf.
9. *Op. cit.,* p. 2.
10. Selon la Smart Card Alliance, « un dispositif utilisant une puce intelligente sans contact comprend un microcontrôleur sécurisé intégré ou une technologie équivalente, une mémoire interne et une petite antenne, et communique par un lecteur au moyen d'une interface de radiofréquence sans contact. L'interface sans contact est utile aux utilisateurs, car elle permet au dispositif sans contact d'être lu sur de courtes distances et de transférer les données rapidement. La technologie de la puce intelligente sans contact est disponible sous diverses formes : cartes plastifiées, montres, porte-clés, documents et autres appareils portatifs tels que les téléphones cellulaires. [traduction] » Smart Card Alliance, *Contactless Chip Technology: The Business Benefits*. En ligne (en anglais seulement) : Smart Card Alliance, http://www.smartcardalliance.org/alliance_activities/contactless_business_benefits.cfm.
11. Smart Card Alliance, « RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities ». En ligne (en anglais seulement) : HID Global, http://www.hidcorp.com/documents/tagsVsSmartcards_wp_en.pdf.
12. Juels, *RFID Security and Privacy*, p. 16, note 8.
13. « Firewall Protection for Paper Documents », *RFID Journal,* 11 février 2004. En ligne (en anglais seulement) : http://rfidjournal.com/article/articleview/790/1/1.
14. Allocution par Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, « Trouver le bon équilibre en ce qui concerne la protection de la vie privée en milieu de travail », atelier de l'Université Ryerson concernant la protection de la vie privée en milieu de travail, 30 novembre 2006. En ligne : http://www.privcom.gc.ca/speech/2006/sp-d_061130_f.asp.

15. Commissariat à la protection de la vie privée du Canada, *Fiche d'information : la protection des renseignements personnels au travail*. En ligne : CPVP, http://www.privcom.gc.ca/fs-fi/02_05_d_17_f.asp.
16. Teresa Scassa et coll., *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies,* avril 2005, p. 48. En ligne (en anglais seulement) : Université Dalhousie, http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf.
17. Edward Balkovich et coll., *9 to 5: Do You Know if Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*, RAND Corporation, 2005, p. 14. En ligne (en anglais seulement) : RAND Corp., http://www.rand.org/pubs/technical_reports/TR197.
18. *Op. cit.*, p. 13–14.
19. IBM, « IBM RFID Solution for Asset Tracking—location awareness and safety ». En ligne (en anglais seulement) : IBM, http://www-03.ibm.com/industries/chemicalspetroleum/doc/content/solution/1518038320.html.
20. « Silent Commerce Has Arrived », *RFID Journal*. En ligne (en anglais seulement) : *RFID Journal,* http://www.rfidjournal.com/magazine/article/767/1/95. Le projet du casino de Sydney est mentionné par Accenture, l'entreprise qui l'a mis en œuvre, dans sa brochure publicitaire. En ligne (en anglais seulement) : Accenture, http://www.accenture.com/NR/rdonlyres/39F0E23D-7ABF-46EB-90C0-63FDB59FDA7A/0/Star_City_Casino_Final.pdf.
21. Cette affaire a été rapportée par de nombreuses sources, y compris par Michael Millar dans « Union calls for halt to RFID tracking of workers », 18 juillet 2005. En ligne (en anglais seulement) : PersonnelToday.com, http://www.personneltoday.com/articles/2005/07/18/30851/union-calls-for-halt-to-rfid-tracking-of-workers.html, et sur le site du syndicat GMB, http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057.
22. Stephanie Perrin, « RFID and Global Privacy Policy », dans Garfinkel, Simson et Rosenberg (dir. publ.), *RFID: Applications, Security, and Privacy*, New Jersey, Pearson Education, 2005, p. 64. En ligne (en anglais seulement) : ID Trail Project, http://idtrail.org/files/Perrin%20-%20RFID%20and%20Global%20Privacy%20Policy.pdf.
23. IBM, « IBM RFID Solution for Asset Tracking—location awareness and safety ». En ligne (en anglais seulement) : IBM, http://www-03.ibm.com/industries/chemicalspetroleum/doc/content/solution/1518038320.html.
24. « Montreal to use GPS to keep tabs on workers », *Toronto Star,* 26 avril 2006, p. A1 et A8.
25. K.C. Jones, « VeriChip wants to test human implantable RFID on military », 23 août 2006. En ligne (en anglais seulement) : TechWeb, http://www.techweb.com/wire/ebiz/192203522.
26. Hitachi, Mu Solutions. En ligne (en anglais seulement) : http://hitachi-eu.com/mu/Products/Mu%20Chip.htm.
27. CBC News, « Hitachi develops powder-sized RFID chips », 23 février 2007. En ligne (en anglais seulement) : http://www.cbc.ca/technology/story/2007/02/23/tech-rfid.html.
28. « Kodak's RFID Moment », *RFID Journal.* En ligne (en anglais seulement) : http://www.rfidjournal.com/article/articleview/3100.
29. Groupe de travail Article 29 sur la protection des données, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, 10107/05/FR, 19 janvier 2005, p. 7–8. En ligne : Europa, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.
30. Lisa Madelon Campbell, « Les nanotechnologies et le plan national américain de recherche et de développement pour la protection des infrastructures critiques », *Canadian Journal of Law and Technology*, vol. 5, n° 3 (novembre 2006). En ligne :

http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook2_FR.html#section003.

31. « Finnair, IBM and Nokia Improve Passenger Service at Helsinki Airport: Radio Frequency Identification Technology Streamlines Airport Ground Handling », communiqué d'IBM, 12 juin 2006. En ligne (en anglais seulement) : IBM, http://www-03.ibm.com/press/us/en/pressrelease/19805.wss.
32. Bob Barr, « The Real Toll is Your Privacy », *The Atlanta Journal Constitution*, 15 août 2007. En ligne (en anglais seulement) : Bob Barr http://www.bobbarr.org/default_print.asp?pt=newsdescr&RI=873.
33. Adaptation de DN-Systems, « RFID: Security Concerns ». En ligne (en anglais seulement) : DN-Systems, http://www.dn-systems.de/technology/RFID/.
34. Annalee Newitz, « The RFID Hacking Underground », *Wired Magazine,* vol. 14, nº 5, mai 2006. En ligne (en anglais seulement) : http://www.wired.com/wired/archive/14.05/rfid.html.
35. Melanie R. Rieback, Bruno Crispo et Andrew S. Tanenbaum, *Is Your Cat Infected With a Computer Virus?*, Computer Systems Group, Vrije Universiteit Amsterdam, 2006. En ligne (en anglais seulement) : Vrije Universiteit, http://www.rfidvirus.org/papers/percom.06.pdf. Voir également : Will Knight, « RFID Worm Created in the Lab », *New Scientist*, 15 mars 2006. En ligne (en anglais seulement) : New Scientist : http://www.newscientisttech.com/channel/tech/dn8854.html.
36. *Loi sur la protection des renseignements personnels*, art. 2 et annexe. Voir l'annexe III du présent document.
37. Secrétariat du Conseil du Trésor du Canada, *Orientation stratégique du gouvernement : gestion de l'information*. En ligne : Conseil du Trésor, http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/im-gi/sdg-osg1_f.asp.
38. Secrétariat du Conseil du Trésor du Canada, *Politique sur la sécurité*. En ligne : Conseil du Trésor, http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp.
39. Secrétariat du Conseil du Trésor du Canada, *Code de la protection des renseignements personnels concernant les employés.* En ligne : http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP3_3_f.asp.
40. Secrétariat du Conseil du Trésor du Canada, Évaluation des facteurs relatifs à la vie privée — Politique et Publications. En ligne : Conseil du Trésor, http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_f.asp.
41. L.O. 2004, ch. 3.
42. Ce terme est défini dans la *LPRPDÉ*. La définition est reproduite à l'annexe III du présent document.
43. *Op. cit.*, art. 2.
44. Par exemple, dans l'affaire *Dagg c. Canada (ministre des Finances),* le juge La Forest indique que : « Comme l'a souligné le juge en chef adjoint Jerome dans *Canada (Commissaire à l'information) c. Canada (Solliciteur général)*, précité, à la p. 557, la formulation de cet article est "délibérément large" et "illustre tout à fait les efforts considérables qui ont été déployés pour protéger l'identité des individus". Elle *semble destinée à viser tout renseignement sur une personne donnée, sous la seule réserve d'exceptions précises [référence omise]. Une telle interprétation s'accorde avec le texte clair de la Loi, avec son historique législatif et avec le statut privilégié et fondamental du droit à la vie privée dans notre culture sociale et juridique.* » *Loi sur la protection des renseignements personnels*, art. 3.
45. *Dagg c. Canada*, [1997] 2 R.C.S. 403. En ligne : LEXUM, http://scc.lexum.umontreal.ca/fr/1997/1997rcs2-403/1997rcs2-403.html.
46. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 319, « Mesures anti-pourriel du FSI contestées », 13 février 2006. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2005/319_20051103_f.asp.

47. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 270, « La banque accepte de changer son message automatisé », 21 juin 2004. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_f.asp.
48. Rapport d'enquête P2005-IR-04, R.J. Hoffman Holdings Ltd., 13 mai 2005. En ligne (en anglais seulement) : Commissariat à l'information et à la protection de la vie privée de l'Alberta, http://www.oipc.ab.ca/media/127893/P2005-004IR.pdf.
49. Rapport d'enquête P2005-IR-009, Precision Drilling Corporation, 4 novembre 2005. En ligne (en anglais seulement) : Commissariat à l'information et à la protection de la vie privée de l'Alberta, http://www.oipc.ab.ca/media/127860/P2005-009IR.pdf.
50. « Mexican university selects AXCESS asset management RFID solution », *More RFID*, 10 mai 2006. En ligne (en anglais seulement) : *More RFID*, http://www.axcessinc.com/knowledge/2006/pr20061004_Mexican_University_AXCESS.pdf.

51. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 220, « Une télévendeuse refuse que son rendement soit communiqué par son employeur à d'autres employés », 19 janvier 2004. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_f.asp.
52. Scassa et coll.
53. Mémoire présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, 22 février 2007. En ligne : CPVP, http://www.privcom.gc.ca/parl/2007/sub_070222_f.asp.
54. *Dagg c. Canada*, [1997] 2 R.C.S. 403. En ligne : LEXUM, http://scc.lexum.umontreal.ca/fr/1997/1997rcs2-403/1997rcs2-403.html.
55. *Personal Information Protection Act*, [SBC 2003] ch. 63, art. 1.
56. Voir, par exemple : *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14; *Ross c. Rosedale Transport Ltd*., [2003] C.L.A.D. nº 237; *Re Canadian Pacific Ltd. et Brotherhood of Maintenance of Way Employees* (1996), 59 L.A.C. (4e) 111.
57. CPVP, note 14 ci-dessus.
58. *Ibid*.
59. Voir, par exemple : *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14; *Ross v. Rosedale Transport Ltd*., [2003] C.L.A.D. nº 237; *Re Canadian Pacific Ltd. et Brotherhood of Maintenance of Way Employees* (1996), 59 L.A.C. (4e) 111.
60. (2004), 16 Admin. L.R. (4e) 275 • (2004), 33 C.P.R. (4e) 1, par. 127.
61. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 279, « La surveillance des employés au travail », 27 septembre 2004. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_f.asp.
62. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 281, « Une organisation utilise la biométrie à des fins d'authentification », 26 octobre 2004. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_f.asp.
63. *Turner c. Telus Communications Inc.*, [2005] C.F. 1601.
64. *Wansink c. Telus Communications Inc.*, [2007] CAF 21.
65. Todd Lewan, « Microchip implants park privacy worry; security measures may lead to tracking », AP repris dans le *Chicago Tribune*, 30 juillet 2007.
66. Évaluation des facteurs relatifs à la vie privée — Politique et Publications, note 37 ci-dessus.
67. *LPRPDÉ*, annexe 1.
68. *LPRPDÉ*, annexe 1, principe 4.1.
69. Commissariat à la protection de la vie privée du Canada, resources en matière d'Évaluations des facteurs relatifs à la vie privée, http://www.privcom.gc.ca/pia-efvp/index_f.asp.

70. Christian Floerkemeier et coll., *Scanning with a Purpose: Supporting the Fair Information Principles in RFID Protocols*, Institute for Pervasive Computing, Suisse, 2004, p. 4. En ligne en anglais seulement) : http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf (également disponible dans Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda et Michiaki Yasumura (dir. publ.), *Ubiquitous Computing Systems: Second International Symposium*, UCS, Tokyo (Japon), 8 et 9 novembre 2004, documents choisis révisés, Berlin, Springer–Verlag, 2005, p. 214–231.
71. *Ibid.*
72. *Ibid.*
73. Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* nº 273, « À la suite de l'installation de caméras de surveillance sur les lieux de travail, une compagnie de radiodiffusion s'engage à informer ses employés des fins de la collecte et à adopter une politique concernant leur utilisation », 21 juin 2004. En ligne : CPVP, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040518_f.asp.
74. 2004 CAF 387. En ligne : Cour d'appel fédérale, http://decisions.fca-caf.gc.ca/fr/2004/2004caf387/2004caf387.html
75. Allocution prononcée par Patricia Kosseim, avocate générale, Commissariat à la protection de la vie privée du Canada, à l'Association canadienne des compagnies d'assurances de personnes, Conférence annuelle conjointe de 2006 de la Section de l'observation et de la Section des agents de plaintes des consommateurs, 11 mai 2006. En ligne : CPVP, http://www.privcom.gc.ca/speech/2006/sp-d_060511_pk_f.asp.
76. *LPRPDÉ*, art. 7(1)(*b*).
77. *Eastmond c. Canadian Pacifique Limitée*, 2004 CF 852, par. 187. En ligne : Cour fédérale du Canada, http://decisions.fct-cf.gc.ca/fr/2004/2004cf852/2004cf852.html. Il convient de souligner, cependant, que la conception particulière du système, c.-à-d. certaines mesures de sécurité et limitations, a joué un rôle dans la décision de la Cour.
78. Floerkemeier et coll., p. 7.
79. *Ibid.*
80. *Op. cit.*, p. 5
81. *Ibid.*
82. *Ibid.*
83. Perrin, note 19 ci-dessus, p. 76.
84. Simson Garfinkel, « Adapting Fair Information Practices to Low-Cost RFID System », dans Simson Garfinkel et Beth Rosenberg (dir. publ.), *RFID: Applications, Security, and Privacy*, New Jersey, Pearson Education, 2005, p. 522.
85. International Commission on Non-Ionizing Radiation Protection, *Possible Health Risks to the General Public from the Use of Security and Similar Devices*, 2002. En ligne (en anglais seulement) : ICNIRP, http://www.icnirp.de/documents/ExSummary.pdf.
86. Adaptation de Perrin, note 21 ci-dessus, p. 79.
87. John Godfrey, cité dans *La vie privée : où se situe la frontière?* Rapport de la Chambre des communes, Comité permanent des droits de la personne et de la condition des personnes handicapées, 1997, p. 16. En ligne : CPVP, http://www.privcom.gc.ca/information/02_06_03d_f.pdf.
88. Fiche d'information, note 14 ci-dessus.
89. Teresa Scassa et coll., « Consumer Privacy and Radio Frequency Identification Technology », *Revue de droit d'Ottawa*, vol. 37, nº 215–248 (2005-2006), p. 218.

90. Simson Garfinkel et Henry Holtzman, « Understanding RFID Technology », dans Simson Garfinkel et Beth Rosenberg (dir. publ.), *RFID: Applications, Security, and Privacy*, New Jersey, Pearson Education, 2005, p. 17.
91. *Op. cit.*, p. 18.