
POLITIQUE SUR L'IDENTIFICATION ET LE TRAITEMENT DES BIENS ET RENSEIGNEMENTS CLASSIFIÉS

But

Conformément à la *Politique de sécurité du gouvernement*, l'Office national du film (l'«ONF») doit protéger la confidentialité, l'intégrité et la disponibilité des renseignements et des biens dont il est responsable. Les renseignements et les biens doivent être identifiés et catégorisés en fonction du degré de préjudices potentiels qui pourraient exister si l'intégrité de ces renseignements et biens était compromise.

La présente politique et les procédures afférentes visent à fournir des normes et lignes directrices pour l'identification, la classification, la catégorisation, le marquage et la protection des biens et renseignements en fonction de leur nature délicate.

La présente politique traite de l'identification et du traitement des renseignements dits «classifiés», c'est-à-dire ceux concernant l'intérêt national. Compte tenu du mandat de l'ONF et de son positionnement au sein du gouvernement canadien, ce type de renseignements est peu susceptible d'être créé ou divulgué à l'ONF. Néanmoins, il est souhaitable de prendre connaissance de la présente politique dans l'éventualité où de tels renseignements seraient en la possession du personnel, de directeurs ou autres personnes à l'ONF.

Veuillez vous référer à la *Politique sur l'identification et le traitement des biens et renseignements protégés* pour toute question relative aux renseignements protégés (c.-à-d. les renseignements confidentiels autres que ceux d'intérêt national).

Champ d'application

Cette politique s'applique à tous les employés, cadres, directeurs, membres du conseil d'administration, sous-traitants, contractuels, pigistes et stagiaires de l'ONF.

Politiques et législations applicables

- Loi sur l'accès à l'information («LAI»)
- Loi sur la protection des renseignements personnels («LPRP»)
- Politique du gouvernement sur la sécurité («PGS»)
- Politique de l'ONF sur la protection des renseignements personnels
- Politique et les procédures relatives à l'identification des biens et renseignements à caractère essentiel
- Politique sur l'identification et le traitement des biens et renseignements protégés

Définitions

- Auteur - Toute personne qui crée ou recueille des renseignements.
- Biens - Éléments d'actifs corporels ou incorporels qui ont de la valeur et qui doivent donc être protégés. Les biens incluent, sans y être limités, les renseignements quels qu'en soient la forme et les supports, les réseaux, les systèmes, le matériel, les biens immobiliers, les ressources financières, la fiabilité des employés, la confiance du public et la réputation internationale. Les biens peuvent être classifiés ou protégés.
- Compromission - Perte ou divulgation, destruction, retrait, modification, interruption ou utilisation non autorisée de renseignements.
- Confidentialité - Caractère attribué aux renseignements qui ne doivent pas être divulgués à des personnes non autorisées, parce qu'il en résulterait un préjudice à l'intérêt national ou à d'autres intérêts.

- Disponibilité - Condition des renseignements qui doivent être utilisables sur demande à l'appui des opérations, des programmes et des services.
- Intégrité - Caractère exact et complet des biens et authenticité des transactions.
- Renseignements – Toute donnée, tout matériel publié ou tout document sous une forme matérielle, qui est recueilli, créé ou reçu et qui est conservé comme preuve dans le cadre des obligations légales ou de transactions d'affaires.
- Renseignements classifiés - Renseignements importants pour l'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* et qui concernent la défense et le maintien de la stabilité sociale, politique et économique du Canada. Cela comprend tous les renseignements qui, si leur intégrité était compromise ou s'ils faisaient l'objet d'une divulgation non autorisée, pourraient raisonnablement causer un préjudice à l'intérêt national.
- Renseignements protégés - Renseignements autres que d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* mais qui requièrent une protection.
- Valeur - Importance monétaire, culturelle, stratégique ou autre.

Énoncé de la politique

L'ONF a comme politique d'assurer une protection adéquate des Biens et Renseignements dont il a la garde en faisant en sorte que l'accès à ceux-ci soit limité aux personnes autorisées ayant besoin d'en prendre connaissance dans le cadre de leurs fonctions.

Objectif de la politique

L'objectif de cette politique est d'assurer la confidentialité des Renseignements et des Biens désignés en tant que Renseignements classifiés de l'ONF.

Précision sur la protection des Biens et des Renseignements de nature délicate

La protection des Biens et des Renseignements de nature délicate s'appuie sur le principe du préjudice, à savoir les conséquences qui découleraient vraisemblablement de toute atteinte qui pourrait leur être portée. Ces conséquences peuvent être de nature diverse, mais elles affectent normalement de manière temporaire ou permanente leur Confidentialité, leur Disponibilité, leur Intégrité, ou dans le cas plus spécifique des Biens, leur Valeur.

Pour des raisons de clarté, cette politique traitera spécifiquement de Confidentialité des Renseignements et des Biens visés par la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*. Les exigences en matière de Disponibilité, d'Intégrité ou de Valeur seront traitées dans la *Politique et les procédures relatives à l'identification des Biens et Renseignements à caractère essentiel*.

Ainsi, par perte de Confidentialité on entend généralement qu'une ou plusieurs personnes non autorisées prennent connaissance de l'existence d'un Bien ou d'un Renseignement de nature délicate, de sa nature, de l'endroit où il se trouve ou encore des fins auxquelles il est utilisé par l'ONF. Par exemple, ce sera le cas de la divulgation fortuite ou délibérée, à une personne extérieure à l'ONF, de données considérées comme étant de la propriété intellectuelle de nature délicate (données confidentielles jusqu'au moment de leur divulgation publique) appartenant au gouvernement ou à un tiers (par exemple, la divulgation d'une invention avant le dépôt d'une demande d'un brevet d'invention) ou encore des informations de nature confidentielle sur la position de l'ONF lors de négociations d'ententes particulières sur la scène nationale ou internationale.

Exigences de la politique

Renseignements classifiés:

Il y a trois catégories de Renseignements classifiés : Très secret, Secret et Confidentiel. La catégorie est établie et cotée selon le degré de préjudice potentiel qui pourrait en résulter si l'Intégrité des Renseignements était compromise : Confidentiel - préjudice; Secret - préjudice grave; Très secret - préjudice exceptionnellement grave. En cas de doute concernant la classification de ces Renseignements, l'Auteur doit se référer aux articles 13 à 26, 68 et 69 de la *Loi sur l'accès à l'information* et aux articles 3 (définition de «renseignements personnels»), 7, 8 et 18 à 28 de la *Loi sur la protection des renseignements personnels*, dont copie est jointe à l'Annexe B.

À titre d'exemple, les articles 13, 14, 15, 16, 21, 68 et 69 de la *Loi sur l'accès à l'information* traitent de Renseignements dont la divulgation est interdite (sauf à certaines conditions), possiblement en raison de l'intérêt national. Les articles 17, 18, 19, 20, 22 et 23 de la *Loi sur l'accès à l'information* traitent des autres types de Renseignements, comprenant les Renseignements protégés qui touchent entre autre, les intérêts d'individus.

Tous les Renseignements classifiés doivent être déclassifiés lorsque le niveau de protection approprié n'est plus nécessaire, conformément à la procédure 10 à l'Annexe A.

Seuls les employés qui possèdent le niveau de sécurité approprié et qui ont besoin de connaître les Renseignements classifiés pour s'acquitter de leurs fonctions peuvent avoir accès à ces Renseignements et aux Biens classifiés. Par conséquent, les employés qui doivent avoir accès à des Renseignements classifiés doivent obtenir une cote de sécurité appropriée de la part des autorités compétentes.

Lorsque les Renseignements ou les Biens classifiés doivent être partagés avec d'autres gouvernements, organismes étrangers, internationaux ou privés, il faudra consulter la Section de la Gestion de l'information (Direction, Planification stratégique et relations gouvernementales) pour s'assurer que les exigences en matière de sécurité aux fins de leur protection soient appliquées. Toute entente permettant le partage de Renseignements classifiés devra préciser les responsabilités particulières des parties en matière de sécurité, les mesures de protection à prendre et à suivre, les procédures de sécurité relatives au partage de ces Renseignements.

Responsabilités

Les Auteurs doivent identifier et catégoriser les Renseignements qu'ils créent ou recueillent, les coter selon le niveau approprié de sécurité, en conformité avec la présente politique et les déclassifier lorsque les mesures de protection visant la catégorie identifiée ne sont plus requises.

Les gestionnaires doivent s'assurer que tous les Renseignements créés ou recueillis dans leur secteur de responsabilité sont identifiés et catégorisés, cotés selon le niveau approprié de sécurité, en conformité avec la présente politique et déclassifiés lorsque les mesures de protection appropriées pour la catégorie identifiée ne sont plus requises. Les gestionnaires doivent également s'assurer que les employés possèdent le niveau de sécurité approprié avant de leur permettre d'avoir accès aux Renseignements classifiés. La Directrice de l'Administration s'occupe d'obtenir les différents niveaux de sécurité auprès des autorités gouvernementales. Le gestionnaire doit lui adresser toute demande à cet effet en justifiant cette demande. L'obtention d'une cote de sécurité pour un employé implique qu'une enquête de la GRC sera faite sur lui et sa famille, incluant la vérification d'antécédents judiciaires.

Interprétation

Toute question relative à l'interprétation et l'application de la présente politique, doit être adressée au Directeur, Relations d'affaires et services juridiques ou à la Coordinatrice ou le Coordonnateur de l'accès à l'information.

Procédures

Les procédures suivantes sont à l'Annexe A de la présente politique et en précisent les modalités d'application :

1. Classification et catégorisation des Biens et des Renseignements en matière de Confidentialité
2. Identification des Biens et des Renseignements en fonction de leur Confidentialité (cote de sécurité)
3. Entreposage des Renseignements classifiés et des Biens classifiés
4. Partage des Renseignements classifiés et des Biens classifiés
5. Transmission des Renseignements classifiés sur support papier
6. Transmission électronique des Renseignements classifiés
7. Transmission par télécopieur des Renseignements classifiés
8. Transmission par téléphone des Renseignements de nature délicate
9. Sortie des Renseignements classifiés
10. Déclassification des Renseignements classifiés
11. Destruction des Renseignements classifiés et des Biens classifiés

Extraits pertinents de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*

Les extraits pertinents de ces deux lois sont à l'Annexe B de la présente politique pour fins de référence.

Annexes A - PROCÉDURES

Procédure 1 - CLASSIFICATION

CLASSIFICATION ET CATÉGORISATION DES BIENS ET DES RENSEIGNEMENTS EN MATIÈRE DE CONFIDENTIALITÉ

Tous les Renseignements et les Biens de l'ONF doivent recevoir une attention appropriée. Toutefois, il y a certains types de Renseignements et de Biens qui sont de nature délicate ou qui ont une certaine Valeur, et auxquels il faut accorder une protection appropriée. Ces Renseignements pourraient causer un préjudice à l'intérêt national ou à un particulier ou à une entreprise si leur Intégrité était compromise. Les dispositions de la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*, dont les extraits pertinents sont à l'Annexe B, établissent l'autorité légale pour refuser l'accès à certains Renseignements, afin de préserver l'intérêt national ou de protéger d'autres intérêts à l'égard desquels le gouvernement a des obligations. Des mesures de sécurité visant l'identification, la manutention, l'entreposage et la destruction de ces Renseignements doivent être appliquées pour protéger ces Renseignements et pour empêcher leur communication, leur modification, leur perte ou leur destruction non autorisée.

Les Auteurs, c'est-à-dire les personnes qui créent un document ou le reçoivent d'un autre organisme sont responsables d'en évaluer la nature délicate et d'y attribuer la cote ou la catégorisation de sécurité appropriée s'il y a lieu et de les déclassifier par la suite.

Confidentialité

Il y a bris de la Confidentialité lorsqu'il y a divulgation sans autorisation de Renseignements classifiés ou de Biens classifiés. Les précautions prises pour assurer la Confidentialité des Renseignements et des Biens comprennent la mise en place de mesures de sécurité pour assurer que l'accès aux Renseignements classifiés et aux Biens classifiés soit limité aux seules personnes qui ont besoin d'y avoir accès ou d'en prendre connaissance dans le cadre de leurs fonctions et qui possèdent la cote de sécurité appropriée.

Au gouvernement fédéral, la Confidentialité se fonde sur les critères d'exceptions et d'exclusions qui sont énoncés dans la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*, et qui établissent l'autorité légale en vertu de laquelle les ministères et institutions qui y sont assujettis peuvent refuser de divulguer certains renseignements. Selon la *Politique du gouvernement sur la sécurité*, les ministères doivent identifier et catégoriser les Renseignements pouvant faire l'objet d'exceptions ou d'exclusions en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, d'après le degré de préjudice que peut causer le bris de Confidentialité. La grande majorité de l'information gouvernementale ne fait pas l'objet d'une exemption ou d'une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, et celle-ci n'est pas normalement concernée par les dispositions concernant l'identification et la catégorisation aux fins de Confidentialité à moins que, par regroupement, elle doive être protégée ou que, par inférence, elle ne compromette la Confidentialité d'autres biens ou renseignements.

En matière de Confidentialité, la *Politique du gouvernement sur la sécurité* divise les Biens et les Renseignements en deux grandes catégories, à savoir :

- ceux dont l'atteinte pourrait causer un préjudice à l'intérêt national ou à la sécurité nationale; et

- ceux dont l'atteinte serait susceptible de causer un préjudice à un intérêt autre que l'intérêt national ou la sécurité nationale.

La présente politique traite de la première catégorie de Renseignements et de Biens, soit ceux concernant l'intérêt national ou la sécurité nationale.

Par intérêt national et sécurité nationale, on entend une menace à l'Intégrité territoriale du Canada, à ses institutions démocratiques, à sa stabilité politique ou socio-économique ou encore à la capacité du Gouvernement du Canada de promouvoir et de défendre les intérêts du pays.

Renseignements classifiés et Biens classifiés

Les Biens et les Renseignements ayant trait à l'intérêt national et la sécurité nationale sont par ailleurs divisés en trois catégories, selon le degré de sévérité des conséquences qu'une atteinte à ceux-ci serait susceptible de causer.

Ces trois catégories de Biens classifiés et Renseignements classifiés sont comme suit :

1) Très secret : catégorie qui sert lorsqu'une atteinte à l'Intégrité d'une quantité très limitée d'informations pourrait logiquement causer un préjudice exceptionnellement grave à l'intérêt national. Cette classification ne devrait servir que très rarement à l'ONF et seulement lorsqu'une atteinte portée à l'Intégrité d'une certaine information pourrait avoir de graves conséquences, immédiates et irréparables, sur la défense, la sécurité, les relations internationales ou les affaires économiques de la nation. Lorsque cette catégorie est retenue, l'expéditeur doit s'assurer que toutes les mesures spéciales connexes sont réellement et complètement justifiées.

Exemples de Biens ou Renseignements classifiés - Très secrets :

- les documents ou le matériel contenant des plans pour la défense de l'ensemble du pays ou de régions stratégiques vitales pour la défense de celui-ci ;
- l'information sur de nouvelles et importantes munitions, y compris des percées scientifiques et techniques significatives directement liées à la défense du pays ;
- de l'information détaillée sur des alliances nouvelles ou éventuelles en matière de défense, de même que sur les plans de défense des nations alliées ;
- les documents politiques importants traitant de questions telles que les négociations de traités ou d'accords ;
- les affaires vitales du renseignement, susceptibles de mettre en péril les sources des renseignements.

2) Secret : catégorie qui sert lorsqu'une atteinte à l'intégrité de l'information pourrait logiquement causer un préjudice grave à l'intérêt national.

Exemples de Biens ou Renseignements classifiés - Secrets :

- les procès-verbaux ou les dossiers de discussions ou de comités du Cabinet, les projets législatifs (avant publication);
- les documents ou le matériel contenant des plans pour la défense de régions et d'installations militaires;
- les documents ou le matériel directement lié aux négociations importantes et en cours avec les puissances étrangères;
- les détails du budget fédéral avant sa publication officielle;
- l'information relative à une puissance étrangère, dont la valeur repose sur la dissimulation de la possession d'un tel document;
- l'information sur d'importantes nouveautés scientifiques et techniques ayant trait à la sécurité nationale;
- l'information sur l'identité ou la composition d'unités scientifiques ou militaires servant dans des opérations comportant des techniques dont l'existence, si elle était connue, serait précieuse pour une puissance étrangère;

- les documents ou le matériel ayant trait à d'importants plans ou négociations du gouvernement avec des gouvernements étrangers;
- l'information vitale pour l'application des lois;
- l'information sur les méthodes et les procédures dont se servent les organismes de sécurité dans l'exécution de leurs tâches.

N.B. L'ONF a dans ses voûtes certains films faits sous l'égide de l'Armée canadienne, du Ministère de la Défense nationale et d'autres autorités gouvernementales. Ces films font l'objet de restrictions quant à leur exploitation. Certains de ces films pourraient être déclassés avec l'autorisation des autorités compétentes. Pour les autres, ils devraient être classifiés avec la cote de sécurité appropriée après consultation avec les autorités compétentes (c'est-à-dire le ministère ou l'organisme qui a commandité le film).

3) Confidentiel : catégorie qui sert lorsqu'une atteinte à l'Intégrité pourrait logiquement causer un préjudice à l'intérêt national.

Exemples de Biens ou Renseignements classifiés - Confidentiels :

- les procès-verbaux ou les dossiers des discussions des comités interministériels, lorsque leur contenu ne relève pas d'une catégorie supérieure;
- les rapports politiques et économiques qui procureraient un avantage à une puissance étrangère, mais qui ne relèvent pas de la catégorie Secret;
- les opinions personnelles de représentants officiels du gouvernement au sujet d'événements publics, mais qui ne sont pas à communiquer;
- l'information dont la divulgation prématurée nuirait aux plans ou aux intentions du gouvernement.

Procédure 2 – IDENTIFICATION ET MARQUAGE

IDENTIFICATION DES BIENS ET DES RENSEIGNEMENTS EN FONCTION DE LEUR CONFIDENTIALITÉ (COTE DE SÉCURITÉ)

L'Auteur d'un document contenant des Renseignements classifiés ou de Biens classifiés est responsable de marquer celui-ci de façon appropriée au moment où il crée ou reçoit.

Le marquage de la cote de sécurité d'un Bien ou d'un Renseignement vise à indiquer aux utilisateurs les mesures de protection qui doivent lui être appliquées. Il assure la promotion d'une protection uniforme lorsque les Biens ou les Renseignements sont partagés ou échangés. Lorsque la cote de sécurité ne peut être inscrite, on devrait mettre au point d'autres moyens, tel que des procédures opérationnelles et des programmes de sensibilisation, pour veiller à ce que ceux qui ont accès au Bien ou au Renseignement connaissent le niveau de protection nécessaire.

Le marquage comprend :

- Le niveau de sensibilité pertinent
- S'il y a lieu, la date ou l'événement auquel la déclassification doit avoir lieu (voir la Procédure 10 sur la Déclassification)

Documents comportant des Renseignements classifiés

Les Renseignements classifiés doivent être marqués comme suit:

- Renseignements Très Secrets: Inscrivez TRÈS SECRET au coin supérieur droit de chaque page et indiquez le nombre total de pages sur toutes les pages. En cas de reproduction, attribuez un numéro complet et unique à chaque exemplaire, inscrivez le numéro sur chaque page et tenez une liste de distribution.

- Renseignements Secrets : Inscrivez SECRET au coin supérieur droit de chaque page. En cas de reproduction numérotez chaque copie, indiquez le numéro de copie sur la page couverture de chaque exemplaire et tenez une liste de distribution.
- Renseignements Confidentiels : Inscrivez CONFIDENTIEL au coin supérieur droit de chaque page du document. En cas de reproduction et si la situation le justifie, contrôlez les copies des documents Confidentiels de la même façon que les documents Secrets.

Exigences additionnelles

Une mise en garde indique que le Renseignement est assujéti à des exigences additionnelles en plus de celles qui seront indiquées par la cote de sécurité (ex. pour les citoyens canadiens seulement). La mise en garde devrait idéalement être indiquée en haut à droite et au-dessus de la cote de sécurité du document.

Marquage des Biens ou Renseignements classifiés contenus sur supports spéciaux

Supports électroniques

Les supports électroniques comprennent mais sans s'y limiter les disques durs amovibles, les CD, DVD, disquettes, les barrettes de mémoire, les rubans magnétiques, les clés USB, etc. Il faut attribuer une classification de sécurité correspondant à la catégorisation du document le plus sensible conservé sur le support électronique. Le marquage de sécurité des documents eux-mêmes doit être visible sur tout écran ou dispositif sur lequel ils sont affichés; les supports sur lesquels ils sont conservés doivent également être marqués à l'extérieur. Dans la mesure du possible, la mention de sécurité doit être lisible par les personnes comme par les machines.

Le coordonnateur de la Sécurité des technologies de l'information (Direction, Administration) peut donner des conseils sur la manière d'annoter les différents supports électroniques.

Graphiques, cartes, dessins, plans

Le niveau de sensibilité doit paraître à côté de la boîte de titre. Les marquages supplémentaires doivent se faire à l'extérieur afin d'être bien visibles lorsque le matériel est plié ou roulé.

Photographies, films cinématographiques et leurs contenants, bandes vidéo, microfiches, négatifs, transparents et diapositives

Doivent être marqués de telle sorte que le destinataire ou l'observateur puisse connaître le niveau de sensibilité du document.

Enregistrements sonores

Au début et à la fin, les enregistrements doivent contenir un énoncé explicite concernant la protection ou la classification du produit en cause afin d'informer la personne qui écoute. Les enregistrements sont entreposés dans des contenants ou sur des bobines sur lesquels paraissent, bien en vue, les marquages de sécurité.

Marquage des ébauches de documents contenant des Renseignements classifiés

Toute ébauche de document contenant des Renseignements classifiés doit se voir attribuer dès le début le même niveau de classification que le document final et être traitée en conséquence.

Procédure 3 - ENTREPOSAGE

ENTREPOSAGE DES RENSEIGNEMENTS CLASSIFIÉS ET DES BIENS CLASSIFIÉS

Toute personne qui s'absente de son poste de travail doit, au préalable, entreposer dans un coffre de sécurité approprié les Renseignements classifiés en sa possession ou dans le cas où elle travaillait sur un ordinateur, elle doit activer son économiseur d'écran muni d'un mot de passe.

Renseignements conservés sur support papier

Les Renseignements classifiés, les Biens classifiés et les contenants dans lesquels ils sont entreposés doivent être conservés dans des aires où l'on exerce un contrôle efficace de l'accès, conformément aux exigences en matière de sécurité de la catégorie (classifié) et du niveau de protection (Confidentiel, Secret ou Très secret) des Biens ou des Renseignements (exemple : la pièce à accès contrôlé des Ressources humaines, la voûte protégée des Services juridiques, l'entrepôt du Service des archives).

Les Renseignements classifiés avec la cote de sécurité «Confidentiel» doivent être entreposés dans des classeurs barrés approuvés par le *Guide d'équipement de sécurité de la GRC* et conservés dans une zone de travail.

Les Renseignements classifiés avec la cote de sécurité «Secret» doivent être entreposés dans des classeurs barrés ou des coffres-forts approuvés par le *Guide d'équipement de sécurité de la GRC* et conservés dans une zone de sécurité ou de haute sécurité.

Les Renseignements classifiés avec la cote de sécurité «Très secret» doivent être entreposés dans des coffres-forts approuvés par le *Guide d'équipement de sécurité de la GRC* et conservés dans une zone de sécurité ou de haute sécurité.

Les Biens de catégorie classifiée, l'argent comptant et les effets négociables doivent être entreposés dans des contenants (c.-à-d. un coffre-fort ou une chambre forte) spécialement approuvés à cette fin par le *Guide d'équipement de sécurité de la GRC*.

Renseignements conservés sur support électronique

Un Renseignement ou un document classifié ne peut être conservé que sur un réseau informatique sécuritaire, respectant les normes du gouvernement à cet effet et ayant été approuvé par le Coordonnateur de la sécurité et les services informatiques de l'ONF. **L'ONF ne possède pas ce type de réseau pour le moment.**

Les Renseignements classifiés doivent donc être conservés sur un support électronique marqué de façon appropriée et conservé comme un document classifié dans un coffre de sécurité approprié.

Un Renseignement classifié ne doit pas être conservé sur le disque dur d'un ordinateur. Lorsque terminé, le document doit être transféré sur un support électronique approprié et conservé dans un classeur rencontrant les critères de protection nécessaires.

Le Spécialiste en sécurité des services informatiques (Direction, Administration) peut donner des conseils sur la manière de protéger des Renseignements classifiés sur support électronique.

Référence

- Le *Catalogue du matériel de sécurité* publié par TPSGC contient la liste du matériel de sécurité approuvé par le *Guide d'équipement de sécurité de la GRC* pour les offres à commandes principales et nationales :
<http://publiservice.gc.ca/services/icpsss-spicsn/security/items-f.html> .

Procédure 4 – PARTAGE DE RENSEIGNEMENTS

PARTAGE DES RENSEIGNEMENTS CLASSIFIÉS ET DES BIENS CLASSIFIÉS

Les Renseignements classifiés et les Biens classifiés ne doivent être partagés qu'avec des personnes ayant un besoin de savoir et détenant une cote de sécurité / fiabilité valide, correspondant à la classification / catégorisation des Biens ou des Renseignements.

Partage de Renseignements de nature délicate avec un auditoire

Toute personne devant transmettre verbalement un Renseignement classifié doit faire preuve d'une grande prudence en s'assurant que chaque personne de l'auditoire détient une cote de sécurité valide appropriée et qu'elle a besoin de savoir. Elle devrait de plus s'assurer que les locaux sont adéquatement protégés pour permettre la transmission d'un tel Renseignement.

Lorsqu'un Renseignement classifié doit être communiqué verbalement, l'auditoire doit être informé de la nature du Renseignement classifié et de la cote de sécurité qui lui est attribuée.

Toute transmission de Renseignements classifiés à un auditoire à l'extérieur de l'ONF devrait être documentée.

Partage de Renseignements classifiés et de Biens classifiés avec d'autres gouvernements ou organismes

Lorsque des Renseignements sont communiqués à d'autres gouvernements ou organismes, le représentant de l'ONF doit s'assurer par l'entremise d'ententes ou de protocoles d'entente que l'organisme applique les mesures de protection administratives, techniques et matérielles nécessaires afin de protéger les Renseignements.

Par ailleurs, les Renseignements que l'ONF reçoit d'autres gouvernements ou organismes doivent être conservés à un niveau approprié basé sur l'intention de leur Auteur et conformément aux ententes ou protocoles d'entente que l'ONF a conclu avec le gouvernement ou l'organisme.

Reproduction et distribution de Renseignements classifiés

Des copies de Renseignements classifiés avec la cote de sécurité Très secrets ne doivent être effectuées et distribuées qu'avec l'approbation de l'Auteur, du destinataire de l'original ou du Directeur de l'un ou l'autre. Un identificateur unique à chacune des copies du document devra être donné et une liste de distribution devra être conservée au dossier. Dans la mesure du possible on devrait exiger le retour des copies et noter leur retour au dossier.

Les Renseignements classifiés avec la cote de sécurité Secrets ne doivent être reproduits et distribués qu'avec l'approbation de l'Auteur, du destinataire de l'original ou du Directeur de l'un ou l'autre. Chaque copie devra être numérotée, on devra indiquer le numéro de la copie sur la page couverture de chaque exemplaire et tenir une liste de distribution au dossier.

La reproduction de Renseignements classifiés avec la cote de sécurité Confidentiels doit être effectuée en gardant en tête que la distribution de ces Renseignements ne doit se faire qu'à des personnes qui possèdent une cote de sécurité de niveau Confidentiel au minimum et qui ont un besoin opérationnel d'avoir accès à ces Renseignements. Si la situation le justifie, on contrôlera les copies des Renseignements classifiés - Confidentiels de la même façon que les Renseignements classifiés - Secrets.

Procédure 5 – TRANSMISSION SUR SUPPORT PAPIER

TRANSMISSION DES RENSEIGNEMENTS CLASSIFIÉS SUR SUPPORT PAPIER

Tout Renseignement classifié doit être adéquatement emballé et identifié afin d'éviter sa perte ou sa divulgation préméditée ou accidentelle au cours de son acheminement.

Pour le courrier interne et pour le courrier envoyé à l'extérieur de l'ONF, utilisez deux enveloppes cachetées. Mettez uniquement la cote de sécurité sur l'enveloppe intérieure. L'adresse doit cependant figurer sur les deux enveloppes. L'enveloppe intérieure devrait également porter la mention suivante : «Ne peut être ouvert que par le destinataire» (dans le cas de Renseignements à la seule intention du destinataire).

Envoyez les documents par messageries prioritaires, par courrier recommandé, par un service de messageries privé, ou par courrier diplomatique. Le transporteur doit fournir une preuve d'envoi, de transport et de livraison.

Pour les Renseignements classifiés avec les cotes de sécurité Très secrets et Secrets, vous devez placer dans l'enveloppe intérieure un accusé de réception et une enveloppe de retour que le destinataire doit signer et renvoyer.

Vous devez conserver une liste des Renseignements classifiés avec la cote de sécurité Très secrets que vous envoyez, et vous devez prévenir le destinataire avant de faire un envoi.

Un employé autorisé qui a une cote de sécurité appropriée peut aussi transporter des Renseignements et des Biens désignés «classifiés» entre les différents bureaux de l'ONF. L'employé doit assurer la sécurité de ces Renseignements et Biens durant leur transport. On doit utiliser une serviette qui peut être verrouillée ou tout autre contenant sécuritaire (avec une étiquette indiquant l'adresse de retour ou le numéro de téléphone en cas de perte), à moins que les Renseignements et Biens soient trop volumineux. Si le véhicule est laissé sans surveillance, il faut s'assurer que les Renseignements et Biens se trouvent dans le coffre verrouillé de l'automobile ou, si cela est impossible, au moins hors de vue dans l'automobile verrouillée.

Procédure 6 – TRANSMISSION ÉLECTRONIQUE

TRANSMISSION ÉLECTRONIQUE DE RENSEIGNEMENTS CLASSIFIÉS

Un Renseignement classifié ne peut être transmis entre ordinateurs qu'à condition que cette transmission se fasse sur un réseau corporatif sécuritaire, respectant les normes du gouvernement et ayant été approuvé par les Services informatiques de l'ONF. De plus on devra s'assurer que le destinataire possède la cote de sécurité appropriée et le besoin de connaître les Renseignements transmis.

Les Renseignements classifiés ne doivent en aucun cas être transmis par courriel à l'extérieur de l'ONF.

Méthodes de chiffrement

Seuls les Services informatiques peuvent définir le type de chiffrement sécuritaire à utiliser pour la transmission de Renseignements de nature délicate à l'ONF.

Procédure 7 – TRANSMISSION PAR TÉLÉCOPIEUR

TRANSMISSION PAR TÉLÉCOPIEUR DES RENSEIGNEMENTS CLASSIFIÉS

Un Renseignement classifié ne doit pas être transmis par un télécopieur conventionnel; ce type de Renseignement ne peut être transmis que par un télécopieur de type sécuritaire. **L'ONF ne dispose pas de télécopieur de type sécuritaire.**

Procédure 8 – TRANSMISSION PAR TÉLÉPHONE

TRANSMISSION PAR TÉLÉPHONE DE RENSEIGNEMENTS DE NATURE DÉLICATE

Téléphone sans fil

On ne doit pas utiliser un téléphone sans fil pour la transmission de Renseignements de nature délicate à moins que celui-ci possède la capacité de chiffrer le message et que le procédé de chiffrement ait été accepté par le Spécialiste en sécurité des services informatiques (Direction, Administration) de l'ONF.

Téléphone régulier

On ne doit pas utiliser un téléphone conventionnel pour la transmission de tout Renseignement de nature délicate.

Procédure 9 - SORTIE

SORTIE DE RENSEIGNEMENTS CLASSIFIÉS

Les Renseignements classifiés, à l'exception des Renseignements classifiés avec la cote de sécurité Très secret, peuvent être temporairement apportés à l'extérieur du lieu de travail par un employé si son superviseur autorisé (directeur), juge que l'avantage de ce faire pour l'ONF est plus important que les risques additionnels que cela entraîne pour la sécurité de ces Renseignements; une telle pratique ne peut avoir lieu qu'aux conditions suivantes :

- dans le cas de Renseignements classifiés avec la cote de sécurité Secret, une autorisation écrite (sous forme de courriel) doit être obtenue au préalable du directeur de sa direction ou du commissaire de l'ONF;
- dans le cas de Renseignements classifiés avec la cote de sécurité Confidentiel, une autorisation écrite (sous forme de courriel) doit être obtenue au préalable du directeur de sa direction ou du commissaire de l'ONF;
- une mallette sécuritaire pour le transport du Renseignement devra être utilisée;
- identifier la durée pour laquelle l'autorisation est valide;
- mentionner clairement les Renseignements auxquels elle s'applique;
- une copie de chacune des autorisations accordées doit être versée au dossier contenant les Renseignements auxquels elle s'applique et y être conservée;

- les dates de départ et de retour des Renseignements en question doivent être contrôlées par la personne ayant accordé l'autorisation;
- une copie du Renseignement emprunté doit être versée au dossier contenant ce Renseignement pour toute la durée de l'emprunt.

Procédure 10 – DÉCLASSIFICATION

DÉCLASSIFICATION DES RENSEIGNEMENTS CLASSIFIÉS

Les Renseignements doivent être cotés «classifiés» seulement pour la période de temps requise.

Les Renseignements classifiés doivent être déclassifiés lorsque la protection n'a plus de raison d'être pour l'intérêt national ou la sécurité nationale.

Les Renseignements que possède l'ONF ne peuvent être déclassifiés que par l'Auteur ou par les utilisateurs après consultation avec l'Auteur, de concert avec l'agent de sécurité du ministère, le Directeur, Relations d'affaires et services juridiques ou de la Coordinatrice ou le Coordonnateur de l'accès à l'information.

Les modifications apportées à l'inscription des cotes de sécurité doivent être faites à l'encre, datées et paraphées par l'autorité responsable de cette modification. Lorsqu'il y a de la documentation à l'appui de la modification, il faut l'indiquer sur le document.

Lorsqu'il y a un protocole d'entente ou une entente entre l'ONF et tout autre gouvernement, ministère ou organisme, les Renseignements doivent être déclassifiés conformément aux conditions de l'entente. Les Renseignements peuvent également être renvoyés au ministère, institution ou gouvernement d'origine aux fins de dé-classification.

La Section de la Gestion de l'information (Direction, Planification stratégique et relations gouvernementales) doit être consultée lorsqu'il y a des discussions concernant la déclassification des Renseignements partagés avec un gouvernement étranger, un organisme international ou une institution dans le cadre d'un protocole d'entente ou d'une entente.

La Section de la Gestion de l'information (Direction, Planification, évaluation et vérification) doit être consultée avant de procéder à la déclassification des Renseignements ayant trait à la sécurité des télécommunications (COMSEC).

Les Auteurs des documents doivent prévoir une déclassification automatique en choisissant, au moment de la création ou de la collecte des Renseignements, une date précise ou un événement particulier relié à la déclassification. Par exemple, on pourrait inscrire sur un document «Confidentiel jusqu'au moment de l'approbation par le Conseil du Trésor».

Dans le cas des documents électroniques une annotation contenant ces mêmes informations doit apparaître sous la cote de sécurité du document.

Une date d'expiration automatique de dix ans devrait s'appliquer aux Renseignements classifiés avec les cotes de sécurité «Secret», «Confidentiel» et «Protégé A», en plus des dates et des événements particuliers qui entraînent leur déclassification. Toutefois, cette date ne s'appliquerait pas aux Renseignements classifiés avec la cote de sécurité «Très secret» ni aux Renseignements protégés avec la cote de sécurité «Protégé B» qui comportent des renseignements personnels d'individus (par exemple, les dossiers médicaux) ou les Renseignements protégés avec la cote de sécurité «Protégé C» (par exemple, les renseignements protégeant les témoins).

Les risques découlant de l'utilisation d'une date d'expiration automatique sont acceptables compte tenu du fait que retirer une classification d'un document n'équivaut pas à rendre le document public. Le processus normal d'examen de toute demande d'accès demeure en vigueur.

Les Renseignements classifiés et les autres Biens classifiés doivent être déclassifiés lorsqu'il est établi que leur divulgation ne poserait aucun risque de préjudice à l'intérêt national ou la sécurité nationale. Ces Renseignements peuvent perdre leur caractère délicat au fil du temps ou lorsque surviennent des événements particuliers. Le fait de retirer une classification d'un document n'équivaut pas à rendre le document public. Le processus normal d'examen de toute demande d'accès demeure en vigueur.

La déclassification de Renseignements ou de Biens à un niveau de classification inférieure doit avoir lieu si le préjudice à l'intérêt national ou la sécurité nationale a diminué. La déclassification à la catégorie Renseignements protégés, avec la cote de sécurité appropriée, peut également avoir lieu s'il n'y a plus de risque de préjudice potentiel à l'intérêt national ou la sécurité nationale, mais qu'il y a encore risque de préjudice à des intérêts privés ou non reliés à l'intérêt national ou la sécurité nationale.

Procédure 11 - DESTRUCTION

DESTRUCTION DES RENSEIGNEMENTS CLASSIFIÉS ET DES BIENS CLASSIFIÉS

Renseignements sur support papier

Les Renseignements classifiés dont la période de conservation est échue ne doivent être détruits que par la Section de la Gestion de l'information (Direction, Planification stratégique et relations gouvernementales) à l'aide de l'une des méthodes suivantes:

- en utilisant une déchiqueteuse approuvée;
- en utilisant les services de destruction du gouvernement.

Renseignements sur support électronique

Les Renseignements sur support électronique dont la période de conservation est échue ne doivent être détruits que par la Section de la Gestion de l'information (Direction, Planification stratégique et relations gouvernementales), en collaboration avec les Services informatiques (Direction, Administration). Si elle ne dispose pas du matériel ou des installations nécessaires, la section de la Gestion de l'information utilisera les services de destruction du gouvernement.

Annexe B – EXTRAITS PERTINENTS DES LOIS

LOI SUR L'ACCÈS À L'INFORMATION (L.R.C. 1985, ch. A-1)

Voici les dispositions pertinentes pour la présente politique :

Renseignements obtenus à titre confidentiel

13. (1) Sous réserve du paragraphe (2), le responsable d'une institution fédérale est tenu de refuser la communication de documents contenant des renseignements obtenus à titre confidentiel :

- a) des gouvernements des États étrangers ou de leurs organismes;
- b) des organisations internationales d'États ou de leurs organismes;
- c) des gouvernements des provinces ou de leurs organismes;
- d) des administrations municipales ou régionales constituées en vertu de lois provinciales ou de leurs organismes;
- e) d'un gouvernement autochtone.

Cas où la divulgence est autorisée

(2) Le responsable d'une institution fédérale peut donner communication de documents contenant des renseignements visés au paragraphe (1) si le gouvernement, l'organisation, l'administration ou l'organisme qui les a fournis :

- a) consent à la communication;
- b) rend les renseignements publics.

Définition de « gouvernement autochtone »

(3) L'expression « gouvernement autochtone » à l'alinéa (1) e) s'entend :

- a) du gouvernement niska'a, au sens de l'Accord définitif niska'a mis en vigueur par la *Loi sur l'Accord définitif niska'a*;
- b) du conseil, au sens de l'Accord d'autonomie gouvernementale de la première nation de Westbank mis en vigueur par la *Loi sur l'autonomie gouvernementale de la première nation de Westbank*;
- c) du gouvernement tlicho, au sens de l'article 2 de la *Loi sur les revendications territoriales et l'autonomie gouvernementale du peuple tlicho*;
- d) du gouvernement nunatsiavut, au sens de l'article 2 de la *Loi sur l'Accord sur les revendications territoriales des Inuit du Labrador*.

L.R. (1985), ch. A-1, art. 13; 2000, ch. 7, art. 21; 2004, ch. 17, art. 16; 2005, ch. 1, art. 97 et 107, ch. 27, art. 16 et 22.

Affaires fédéro- provinciales

14. Le responsable d'une institution fédérale peut refuser la communication de documents contenant des renseignements dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite par le gouvernement du Canada des affaires fédéro-provinciales, notamment des renseignements sur :

- a) des consultations ou délibérations fédéro-provinciales;
- b) les orientations ou mesures adoptées ou à adopter par le gouvernement du Canada touchant la conduite des affaires fédéro-provinciales.

1980-81-82-83, ch. 111, ann. I « 14 ».

Affaires

15. (1) Le responsable d'une institution fédérale peut refuser la communication de documents contenant des

internationales et défense renseignements dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales, à la défense du Canada ou d'États alliés ou associés avec le Canada ou à la détection, à la prévention ou à la répression d'activités hostiles ou subversives, notamment :

- a) des renseignements d'ordre tactique ou stratégique ou des renseignements relatifs aux manoeuvres et opérations destinées à la préparation d'hostilités ou entreprises dans le cadre de la détection, de la prévention ou de la répression d'activités hostiles ou subversives;
- b) des renseignements concernant la quantité, les caractéristiques, les capacités ou le déploiement des armes ou des matériels de défense, ou de tout ce qui est conçu, mis au point, produit ou prévu à ces fins;
- c) des renseignements concernant les caractéristiques, les capacités, le rendement, le potentiel, le déploiement, les fonctions ou le rôle des établissements de défense, des forces, unités ou personnels militaires ou des personnes ou organisations chargées de la détection, de la prévention ou de la répression d'activités hostiles ou subversives;
- d) des éléments d'information recueillis ou préparés aux fins du renseignement relatif à :
 - (i) la défense du Canada ou d'États alliés ou associés avec le Canada,
 - (ii) la détection, la prévention ou la répression d'activités hostiles ou subversives;
- e) des éléments d'information recueillis ou préparés aux fins du renseignement relatif aux États étrangers, aux organisations internationales d'États ou aux citoyens étrangers et utilisés par le gouvernement du Canada dans le cadre de délibérations ou consultations ou dans la conduite des affaires internationales;
- f) des renseignements concernant les méthodes et le matériel technique ou scientifique de collecte, d'analyse ou de traitement des éléments d'information visés aux alinéas d) et e), ainsi que des renseignements concernant leurs sources;
- g) des renseignements concernant les positions adoptées ou envisagées, dans le cadre de négociations internationales présentes ou futures, par le gouvernement du Canada, les gouvernements d'États étrangers ou les organisations internationales d'États;
- h) des renseignements contenus dans la correspondance diplomatique échangée avec des États étrangers ou des organisations internationales d'États, ou dans la correspondance officielle échangée avec des missions diplomatiques ou des postes consulaires canadiens;
- i) des renseignements relatifs à ceux des réseaux de communications et des procédés de cryptographie du Canada ou d'États étrangers qui sont utilisés dans les buts suivants :
 - (i) la conduite des affaires internationales,
 - (ii) la défense du Canada ou d'États alliés ou associés avec le Canada,
 - (iii) la détection, la prévention ou la répression d'activités hostiles ou subversives.

Définitions

(2) Les définitions qui suivent s'appliquent au présent article.

« activités
hostiles ou
subversives »
“ *subversive or
hostile activities*
”

« activités hostiles ou subversives »

- a) L'espionnage dirigé contre le Canada ou des États alliés ou associés avec le Canada;
- b) le sabotage;
- c) les activités visant la perpétration d'actes de terrorisme, y compris les détournements de moyens de transport, contre le Canada ou un État étranger ou sur leur territoire;
- d) les activités visant un changement de gouvernement au Canada ou sur le territoire d'États étrangers par l'emploi de moyens criminels, dont la force ou la violence, ou par l'incitation à l'emploi de ces moyens;
- e) les activités visant à recueillir des éléments d'information aux fins du renseignement relatif au Canada ou aux

États qui sont alliés ou associés avec lui;

f) les activités destinées à menacer, à l'étranger, la sécurité des citoyens ou des fonctionnaires fédéraux canadiens ou à mettre en danger des biens fédéraux situés à l'étranger.

« défense du Canada ou d'États alliés ou associés avec le Canada »
“ defence of Canada or any state allied or associated with Canada ”

« défense du Canada ou d'États alliés ou associés avec le Canada » Sont assimilés à la défense du Canada ou d'États alliés ou associés avec le Canada les efforts déployés par le Canada et des États étrangers pour détecter, prévenir ou réprimer les activités entreprises par des États étrangers en vue d'une attaque réelle ou éventuelle ou de la perpétration d'autres actes d'agression contre le Canada ou des États alliés ou associés avec le Canada.

1980-81-82-83, ch. 111, ann. I « 15 ».

Enquêtes

16. (1) Le responsable d'une institution fédérale peut refuser la communication de documents :

a) datés de moins de vingt ans lors de la demande et contenant des renseignements obtenus ou préparés par une institution fédérale, ou par une subdivision d'une institution, qui constitue un organisme d'enquête déterminé par règlement, au cours d'enquêtes licites ayant trait :

(i) à la détection, la prévention et la répression du crime,

(ii) aux activités destinées à faire respecter les lois fédérales ou provinciales,

(iii) aux activités soupçonnées de constituer des menaces envers la sécurité du Canada au sens de la *Loi sur le Service canadien du renseignement de sécurité*;

b) contenant des renseignements relatifs à des techniques d'enquêtes ou à des projets d'enquêtes licites déterminées;

c) contenant des renseignements dont la divulgation risquerait vraisemblablement de nuire aux activités destinées à faire respecter les lois fédérales ou provinciales ou au déroulement d'enquêtes licites, notamment :

(i) des renseignements relatifs à l'existence ou à la nature d'une enquête déterminée,

(ii) des renseignements qui permettraient de remonter à une source de renseignements confidentielle,

(iii) des renseignements obtenus ou préparés au cours d'une enquête;

d) contenant des renseignements dont la divulgation risquerait vraisemblablement de nuire à la sécurité des établissements pénitentiaires.

Méthodes de protection, etc.

(2) Le responsable d'une institution fédérale peut refuser la communication de documents contenant des renseignements dont la communication risquerait vraisemblablement de faciliter la perpétration d'infractions, notamment :

a) des renseignements sur les méthodes ou techniques utilisées par les criminels;

b) des renseignements techniques concernant des armes actuelles ou futures;

c) des renseignements portant sur la vulnérabilité de certains bâtiments ou ouvrages ou de réseaux ou systèmes divers, y compris des réseaux ou systèmes informatisés ou de communications, ou portant sur les méthodes employées pour leur protection.

Fonctions de police provinciale ou municipale

(3) Le responsable d'une institution fédérale est tenu de refuser la communication des documents contenant des renseignements obtenus ou préparés par la Gendarmerie royale du Canada, dans l'exercice de fonctions de police provinciale ou municipale qui lui sont conférées par une entente conclue sous le régime de l'article 20 de la *Loi sur la Gendarmerie royale du Canada*, si, à la demande de la province ou de la municipalité, le gouvernement du Canada a consenti à ne pas divulguer ces renseignements.

Définition de
« enquête »

(4) Pour l'application des alinéas (1)*b*) et *c*), « enquête » s'entend de celle qui :

- a*) se rapporte à l'application d'une loi fédérale;
- b*) est autorisée sous le régime d'une loi fédérale;
- c*) fait partie d'une catégorie d'enquêtes précisée dans les règlements.

1980-81-82-83, ch. 111, ann. I « 16 »; 1984, ch. 21, art. 70.

Sécurité des
individus

17. Le responsable d'une institution fédérale peut refuser la communication de documents contenant des renseignements dont la divulgation risquerait vraisemblablement de nuire à la sécurité des individus.

1980-81-82-83, ch. 111, ann. I « 17 ».

Intérêts
économiques du
Canada

18. Le responsable d'une institution fédérale peut refuser la communication de documents contenant :

- a*) des secrets industriels ou des renseignements financiers, commerciaux, scientifiques ou techniques appartenant au gouvernement du Canada ou à une institution fédérale et ayant une valeur importante ou pouvant vraisemblablement en avoir une;
- b*) des renseignements dont la divulgation risquerait vraisemblablement de nuire à la compétitivité d'une institution fédérale;
- c*) des renseignements techniques ou scientifiques obtenus grâce à des recherches par un cadre ou employé d'une institution fédérale et dont la divulgation risquerait vraisemblablement de priver cette personne de sa priorité de publication;
- d*) des renseignements dont la divulgation risquerait vraisemblablement de porter un préjudice appréciable aux intérêts financiers du gouvernement du Canada ou à sa capacité de gérer l'économie du pays, ainsi que ceux dont la divulgation risquerait vraisemblablement de causer des avantages injustifiés à une personne. Ces renseignements peuvent notamment porter sur :
 - (i) la monnaie canadienne, son monnayage ou son pouvoir libératoire,
 - (ii) les projets de changement du taux d'intérêt bancaire ou du taux d'emprunt du gouvernement,
 - (iii) les projets de changement des taux tarifaires, des taxes, impôts ou droits ou des autres sources de revenu,
 - (iv) les projets de changement dans le mode de fonctionnement des institutions financières,
 - (v) les projets de vente ou d'achat de valeurs mobilières ou de devises canadiennes ou étrangères,
 - (vi) les projets de vente ou d'acquisition de terrains ou autres biens.

1980-81-82-83, ch. 111, ann. I « 18 ».

Renseignements
personnels

19. (1) Sous réserve du paragraphe (2), le responsable d'une institution fédérale est tenu de refuser la communication de documents contenant les renseignements personnels visés à l'article 3 de la *Loi sur la protection des renseignements personnels*.

Cas où la
divulgence est
autorisée

(2) Le responsable d'une institution fédérale peut donner communication de documents contenant des renseignements personnels dans les cas où :

- a*) l'individu qu'ils concernent y consent;
- b*) le public y a accès;
- c*) la communication est conforme à l'article 8 de la *Loi sur la protection des renseignements personnels*.

Renseignements
de tiers

20. (1) Le responsable d'une institution fédérale est tenu, sous réserve des autres dispositions du présent article, de refuser la communication de documents contenant :

- a) des secrets industriels de tiers;
- b) des renseignements financiers, commerciaux, scientifiques ou techniques fournis à une institution fédérale par un tiers, qui sont de nature confidentielle et qui sont traités comme tels de façon constante par ce tiers;
- c) des renseignements dont la divulgation risquerait vraisemblablement de causer des pertes ou profits financiers appréciables à un tiers ou de nuire à sa compétitivité;
- d) des renseignements dont la divulgation risquerait vraisemblablement d'entraver des négociations menées par un tiers en vue de contrats ou à d'autres fins.

Essais de
produits ou
essais
d'environnement

(2) Le paragraphe (1) n'autorise pas le responsable d'une institution fédérale à refuser la communication de la partie d'un document qui donne les résultats d'essais de produits ou d'essais d'environnement effectués par une institution fédérale ou pour son compte, sauf si les essais constituent une prestation de services fournis à titre onéreux mais non destinés à une institution fédérale.

Méthodes
utilisées pour les
essais

(3) Dans les cas où, à la suite d'une demande, il communique, en tout ou en partie, un document qui donne les résultats d'essais de produits ou d'essais d'environnement, le responsable d'une institution fédérale est tenu d'y joindre une note explicative des méthodes utilisées pour effectuer les essais.

Essais
préliminaires

(4) Pour l'application du présent article, les résultats d'essais de produits ou d'essais d'environnement ne comprennent pas les résultats d'essais préliminaires qui ont pour objet la mise au point de méthodes d'essais.

Communication
autorisée

(5) Le responsable d'une institution fédérale peut communiquer tout document contenant les renseignements visés au paragraphe (1) si le tiers que les renseignements concernent y consent.

Communication
dans l'intérêt
public

(6) Le responsable d'une institution fédérale peut communiquer, en tout ou en partie, tout document contenant les renseignements visés aux alinéas (1)*b*), *c*) et *d*) pour des raisons d'intérêt public concernant la santé et la sécurité publiques ainsi que la protection de l'environnement; les raisons d'intérêt public doivent de plus justifier nettement les conséquences éventuelles de la communication pour un tiers : pertes ou profits financiers, atteintes à sa compétitivité ou entraves aux négociations qu'il mène en vue de contrats ou à d'autres fins.

Avis, etc.

21. (1) Le responsable d'une institution fédérale peut refuser la communication de documents datés de moins de vingt ans lors de la demande et contenant :

- a) des avis ou recommandations élaborés par ou pour une institution fédérale ou un ministre;
- b) des comptes rendus de consultations ou délibérations où sont concernés des cadres ou employés d'une institution fédérale, un ministre ou son personnel;
- c) des projets préparés ou des renseignements portant sur des positions envisagées dans le cadre de négociations menées ou à mener par le gouvernement du Canada ou en son nom, ainsi que des renseignements portant sur les considérations qui y sont liées;
- d) des projets relatifs à la gestion du personnel ou à l'administration d'une institution fédérale et qui n'ont pas encore été mis en oeuvre.

Décisions

(2) Le paragraphe (1) ne s'applique pas aux documents contenant :

- a) le compte rendu ou l'exposé des motifs d'une décision qui est prise dans l'exercice d'un pouvoir discrétionnaire ou rendue dans l'exercice d'une fonction judiciaire ou quasi judiciaire et qui touche les droits d'une personne;

b) le rapport établi par un consultant ou conseiller à une époque où il n'appartenait pas au personnel d'une institution fédérale ou d'un ministre.

1980-81-82-83, ch. 111, ann. I « 21 ».

Examens et vérifications

22. Le responsable d'une institution fédérale peut refuser la communication de documents contenant des renseignements relatifs à certaines opérations — essais, épreuves, examens, vérifications —, ou aux méthodes et techniques employées pour les effectuer, et dont la divulgation nuirait à l'exploitation de ces opérations ou fausserait leurs résultats.

1980-81-82-83, ch. 111, ann. I « 22 ».

Secret professionnel des avocats

23. Le responsable d'une institution fédérale peut refuser la communication de documents contenant des renseignements protégés par le secret professionnel qui lie un avocat à son client.

1980-81-82-83, ch. 111, ann. I « 23 ».

Interdictions fondées sur d'autres lois

Examen des dispositions interdisant la communication

24. (1) Le responsable d'une institution fédérale est tenu de refuser la communication de documents contenant des renseignements dont la communication est restreinte en vertu d'une disposition figurant à l'annexe II.

(2) Le comité prévu à l'article 75 examine toutes les dispositions figurant à l'annexe II et dépose devant le Parlement un rapport portant sur la nécessité de ces dispositions, ou sur la mesure dans laquelle elles doivent être conservées, au plus tard le 1^{er} juillet 1986, ou, si le Parlement ne siège pas, dans les quinze premiers jours de séance ultérieurs.

1980-81-82-83, ch. 111, ann. I « 24 ».

Prélèvements

25. Le responsable d'une institution fédérale, dans les cas où il pourrait, vu la nature des renseignements contenus dans le document demandé, s'autoriser de la présente loi pour refuser la communication du document, est cependant tenu, nonobstant les autres dispositions de la présente loi, d'en communiquer les parties dépourvues des renseignements en cause, à condition que le prélèvement de ces parties ne pose pas de problèmes sérieux.

1980-81-82-83, ch. 111, ann. I « 25 ».

Refus de communication en cas de publication

26. Le responsable d'une institution fédérale peut refuser la communication totale ou partielle d'un document s'il a des motifs raisonnables de croire que le contenu du document sera publié en tout ou en partie par une institution fédérale, un mandataire du gouvernement du Canada ou un ministre dans les quatre-vingt-dix jours suivant la demande ou dans tel délai supérieur entraîné par les contraintes de l'impression ou de la traduction en vue de l'impression.

1980-81-82-83, ch. 111, ann. I « 26 ».

Non-application de la loi

68. La présente loi ne s'applique pas aux documents suivants :

a) les documents publiés ou mis en vente dans le public;

b) les documents de bibliothèque ou de musée conservés uniquement à des fins de référence ou d'exposition pour le public;

c) les documents déposés à Bibliothèque et Archives du Canada, au Musée des beaux-arts du Canada, au Musée canadien des civilisations, au Musée canadien de la nature ou au Musée national des sciences et de la technologie par des personnes ou organisations extérieures aux institutions fédérales ou pour ces personnes ou organisations.

L.R. (1985), ch. A-1, art. 68; L.R. (1985), ch. 1 (3^e suppl.), art. 12; 1990, ch. 3, art. 32; 1992, ch. 1, art. 143(A); 2004, ch. 11, art. 22.

Documents confidentiels du Conseil privé de la Reine pour le Canada

69. (1) La présente loi ne s'applique pas aux documents confidentiels du Conseil privé de la Reine pour le Canada, notamment aux :

a) notes destinées à soumettre des propositions ou recommandations au Conseil;

- b)* documents de travail destinés à présenter des problèmes, des analyses ou des options politiques à l'examen du Conseil;
- c)* ordres du jour du Conseil ou procès-verbaux de ses délibérations ou décisions;
- d)* documents employés en vue ou faisant état de communications ou de discussions entre ministres sur des questions liées à la prise des décisions du gouvernement ou à la formulation de sa politique;
- e)* documents d'information à l'usage des ministres sur des questions portées ou qu'il est prévu de porter devant le Conseil, ou sur des questions qui font l'objet des communications ou discussions visées à l'alinéa *d)*;
- f)* avant-projets de loi ou projets de règlement;
- g)* documents contenant des renseignements relatifs à la teneur des documents visés aux alinéas *a)* à *f)*.

Définition de
« Conseil »

(2) Pour l'application du paragraphe (1), « Conseil » s'entend du Conseil privé de la Reine pour le Canada, du Cabinet et de leurs comités respectifs.

Exception

(3) Le paragraphe (1) ne s'applique pas :

a) aux documents confidentiels du Conseil privé de la Reine pour le Canada dont l'existence remonte à plus de vingt ans;

b) aux documents de travail visés à l'alinéa (1)*b)*, dans les cas où les décisions auxquelles ils se rapportent ont été rendues publiques ou, à défaut de publicité, ont été rendues quatre ans auparavant.

L.R. (1985), ch. A-1, art. 69; 1992, ch. 1, art. 144(F).

LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (L.R.C. 1985 ch. P-23)

Voici les dispositions pertinentes pour la présente politique :

Définitions

3. Les définitions qui suivent s'appliquent à la présente loi.

« renseignements
personnels »
“ *personal
information* ”

« renseignements personnels » Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :

- a)* les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;
- b)* les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé;
- c)* tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre;
- d)* son adresse, ses empreintes digitales ou son groupe sanguin;
- e)* ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement;
- f)* toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur;

g) les idées ou opinions d'autrui sur lui;

h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions;

i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet;

toutefois, il demeure entendu que, pour l'application des articles 7, 8 et 26, et de l'article 19 de la *Loi sur l'accès à l'information*, les renseignements personnels ne comprennent pas les renseignements concernant :

j) un cadre ou employé, actuel ou ancien, d'une institution fédérale et portant sur son poste ou ses fonctions, notamment :

(i) le fait même qu'il est ou a été employé par l'institution,

(ii) son titre et les adresse et numéro de téléphone de son lieu de travail,

(iii) la classification, l'éventail des salaires et les attributions de son poste,

(iv) son nom lorsque celui-ci figure sur un document qu'il a établi au cours de son emploi,

(v) les idées et opinions personnelles qu'il a exprimées au cours de son emploi;

k) un individu qui, au titre d'un contrat, assure ou a assuré la prestation de services à une institution fédérale et portant sur la nature de la prestation, notamment les conditions du contrat, le nom de l'individu ainsi que les idées et opinions personnelles qu'il a exprimées au cours de la prestation;

l) des avantages financiers facultatifs, notamment la délivrance d'un permis ou d'une licence accordés à un individu, y compris le nom de celui-ci et la nature précise de ces avantages;

m) un individu décédé depuis plus de vingt ans.

Usage des
renseignements
personnels

7. À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :

a) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins;

b) qu'aux fins auxquelles ils peuvent lui être communiqués en vertu du paragraphe 8(2).

1980-81-82-83, ch. 111, ann. II « 7 ».

Communication
des
renseignements
personnels

Cas
d'autorisation

8. (1) Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article.

(2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

a) communication aux fins auxquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins;

b) communication aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication;

c) communication exigée par *subpoena*, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme

ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de renseignements;

d) communication au procureur général du Canada pour usage dans des poursuites judiciaires intéressant la Couronne du chef du Canada ou le gouvernement fédéral;

e) communication à un organisme d'enquête déterminé par règlement et qui en fait la demande par écrit, en vue de faire respecter des lois fédérales ou provinciales ou pour la tenue d'enquêtes licites, pourvu que la demande précise les fins auxquelles les renseignements sont destinés et la nature des renseignements demandés;

f) communication aux termes d'accords ou d'ententes conclus d'une part entre le gouvernement du Canada ou l'un de ses organismes et, d'autre part, le gouvernement d'une province ou d'un État étranger, une organisation internationale d'États ou de gouvernements, le conseil de la première nation de Westbank, ou l'un de leurs organismes, en vue de l'application des lois ou pour la tenue d'enquêtes licites;

g) communication à un parlementaire fédéral en vue d'aider l'individu concerné par les renseignements à résoudre un problème;

h) communication pour vérification interne au personnel de l'institution ou pour vérification comptable au bureau du contrôleur général ou à toute personne ou tout organisme déterminé par règlement;

i) communication à Bibliothèque et Archives du Canada pour dépôt;

j) communication à toute personne ou à tout organisme, pour des travaux de recherche ou de statistique, pourvu que soient réalisées les deux conditions suivantes :

(i) le responsable de l'institution est convaincu que les fins auxquelles les renseignements sont communiqués ne peuvent être normalement atteintes que si les renseignements sont donnés sous une forme qui permette d'identifier l'individu qu'ils concernent,

(ii) la personne ou l'organisme s'engage par écrit auprès du responsable de l'institution à s'abstenir de toute communication ultérieure des renseignements tant que leur forme risque vraisemblablement de permettre l'identification de l'individu qu'ils concernent;

k) communication à tout gouvernement autochtone, association d'autochtones, bande d'Indiens, institution fédérale ou subdivision de celle-ci, ou à leur représentant, en vue de l'établissement des droits des peuples autochtones ou du règlement de leurs griefs;

l) communication à toute institution fédérale en vue de joindre un débiteur ou un créancier de Sa Majesté du chef du Canada et de recouvrer ou d'acquitter la créance;

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(i) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée,

(ii) l'individu concerné en tirerait un avantage certain.

Communication
par Bibliothèque
et Archives du
Canada

(3) Sous réserve des autres lois fédérales, les renseignements personnels qui relèvent de Bibliothèque et Archives du Canada et qui y ont été versés pour dépôt ou à des fins historiques par une institution fédérale peuvent être communiqués conformément aux règlements pour des travaux de recherche ou de statistique.

Copie des
demandes faites
en vertu de l'al.
(2)*e*)

(4) Le responsable d'une institution fédérale conserve, pendant la période prévue par les règlements, une copie des demandes reçues par l'institution en vertu de l'alinéa (2)*e*) ainsi qu'une mention des renseignements communiqués et, sur demande, met cette copie et cette mention à la disposition du Commissaire à la protection de la vie privée.

Avis de
communication
dans le cas de
l'al. (2)*m*)

(5) Dans le cas prévu à l'alinéa (2)*m*), le responsable de l'institution fédérale concernée donne un préavis écrit de la communication des renseignements personnels au Commissaire à la protection de la vie privée si les circonstances le justifient; sinon, il en avise par écrit le Commissaire immédiatement après la communication. La décision de mettre au courant l'individu concerné est laissée à l'appréciation du Commissaire.

Définition de
« bande
d'Indiens »

(6) L'expression « bande d'Indiens » à l'alinéa (2)k) désigne :

a) soit une bande au sens de la *Loi sur les Indiens*;

b) soit une bande au sens de la *Loi sur les Cris et les Naskapis du Québec*, chapitre 18 des Statuts du Canada de 1984;

c) soit la bande au sens de la *Loi sur l'autonomie gouvernementale de la bande indienne sechelte*, chapitre 27 des Statuts du Canada de 1986;

d) la première nation dont le nom figure à l'annexe II de la *Loi sur l'autonomie gouvernementale des premières nations du Yukon*.

Définition de
« gouvernement
autochtone »

(7) L'expression « gouvernement autochtone » à l'alinéa (2) k) s'entend :

a) du gouvernement niska'a, au sens de l'Accord définitif niska'a mis en vigueur par la *Loi sur l'Accord définitif niska'a*;

b) du conseil de la première nation de Westbank;

c) du gouvernement tlicho, au sens de l'article 2 de la *Loi sur les revendications territoriales et l'autonomie gouvernementale du peuple tlicho*;

d) du gouvernement nunatsiavut, au sens de l'article 2 de la *Loi sur l'Accord sur les revendications territoriales des Inuit du Labrador*.

Définition de
« conseil de la
première nation
de Westbank »

(8) L'expression « conseil de la première nation de Westbank » aux alinéas (2)f) et (7)b) s'entend du conseil au sens de l'Accord d'autonomie gouvernementale de la première nation de Westbank mis en vigueur par la *Loi sur l'autonomie gouvernementale de la première nation de Westbank*.

L.R. (1985), ch. P-21, art. 8; L.R. (1985), ch. 20 (2^e suppl.), art. 13, ch. 1 (3^e suppl.), art. 12; 1994, ch. 35, art. 39; 2000, ch. 7, art. 26; 2004, ch. 11, art. 37, ch. 17, art. 18; 2005, ch. 1, art. 106 et 109, ch. 27, art. 21 et 25.

Fichiers
inconsultables

18. (1) Le gouverneur en conseil peut, par décret, classer parmi les fichiers de renseignements personnels inconsultables, dénommés fichiers inconsultables dans la présente loi, ceux qui sont formés de dossiers dans chacun desquels dominent les renseignements visés aux articles 21 ou 22.

Autorisation de
refuser

(2) Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui sont versés dans des fichiers inconsultables.

Éléments que
doit contenir le
décret

(3) Tout décret pris en vertu du paragraphe (1) doit porter :

a) une mention de l'article sur lequel il se fonde;

b) de plus, dans le cas d'un fichier de renseignements personnels formé de dossiers dans chacun desquels dominent des renseignements visés au sous-alinéa 22(1)a)(ii), la mention de la loi dont il s'agit.

1980-81-82-83, ch. 111, ann. II « 18 ».

Renseignements
personnels
obtenus à titre
confidentiel

19. (1) Sous réserve du paragraphe (2), le responsable d'une institution fédérale est tenu de refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui ont été obtenus à titre confidentiel :

a) des gouvernements des États étrangers ou de leurs organismes;

b) des organisations internationales d'États ou de leurs organismes;

c) des gouvernements provinciaux ou de leurs organismes;

d) des administrations municipales ou régionales constituées en vertu de lois provinciales ou de leurs organismes;

e) du conseil, au sens de l'Accord d'autonomie gouvernementale de la première nation de Westbank mis en vigueur par la *Loi sur l'autonomie gouvernementale de la première nation de Westbank*.

Cas où la divulgation est autorisée

(2) Le responsable d'une institution fédérale peut donner communication des renseignements personnels visés au paragraphe (1) si le gouvernement, l'organisation, l'administration ou l'organisme qui les a fournis :

a) consent à la communication;

b) rend les renseignements publics.

L.R. (1985), ch. P-21, art. 19; 2004, ch. 17, art. 19.

Affaires fédéro-provinciales

20. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite par le gouvernement du Canada des affaires fédéro-provinciales.

1980-81-82-83, ch. 111, ann. II « 20 ».

Affaires internationales et défense

21. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales, à la défense du Canada ou d'États alliés ou associés avec le Canada, au sens du paragraphe 15(2) de la *Loi sur l'accès à l'information*, ou à ses efforts de détection, de prévention ou de répression d'activités hostiles ou subversives, au sens du paragraphe 15(2) de la même loi, notamment les renseignements visés à ses alinéas 15(1)a) à i).

1980-81-82-83, ch. 111, ann. II « 21 ».

Enquêtes

22. (1) Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) :

a) soit qui remontent à moins de vingt ans lors de la demande et qui ont été obtenus ou préparés par une institution fédérale, ou par une subdivision d'une institution, qui constitue un organisme d'enquête déterminé par règlement, au cours d'enquêtes licites ayant trait :

(i) à la détection, la prévention et la répression du crime,

(ii) aux activités destinées à faire respecter les lois fédérales ou provinciales,

(iii) aux activités soupçonnées de constituer des menaces envers la sécurité du Canada au sens de la *Loi sur le Service canadien du renseignement de sécurité*;

b) soit dont la divulgation risquerait vraisemblablement de nuire aux activités destinées à faire respecter les lois fédérales ou provinciales ou au déroulement d'enquêtes licites, notamment :

(i) des renseignements relatifs à l'existence ou à la nature d'une enquête déterminée,

(ii) des renseignements qui permettraient de remonter à une source de renseignements confidentielle,

(iii) des renseignements obtenus ou préparés au cours d'une enquête;

c) soit dont la divulgation risquerait vraisemblablement de nuire à la sécurité des établissements pénitentiaires.

Fonctions de police provinciale ou municipale

(2) Le responsable d'une institution fédérale est tenu de refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui ont été obtenus ou préparés par la Gendarmerie royale du Canada, dans l'exercice de fonctions de police provinciale ou municipale, qui lui sont conférées par une entente conclue sous le régime de l'article 20 de la *Loi sur la Gendarmerie royale du Canada*, si, à la demande de la province ou de la municipalité, le gouvernement du Canada a consenti à ne pas divulguer ces renseignements.

Définition de
« enquête »

(3) Pour l'application de l'alinéa (1)b), « enquête » s'entend de celle qui :

- a) se rapporte à l'application d'une loi fédérale;
- b) est autorisée sous le régime d'une loi fédérale;
- c) fait partie d'une catégorie d'enquêtes précisée dans les règlements.

1980-81-82-83, ch. 111, ann. II « 22 »; 1984, ch. 21, art. 90.

Enquêtes de
sécurité

23. Le responsable d'une institution fédérale peut, dans les cas où leur communication risquerait vraisemblablement d'entraîner la divulgation de l'identité de l'informateur à l'origine des renseignements en question, refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) et qui ont été recueillis ou préparés, par un organisme d'enquête déterminé par règlement, lors des enquêtes de sécurité :

- a) qu'exige le gouvernement fédéral ou une institution fédérale à l'égard des individus qu'ils emploient ou qu'emploient des personnes ou organismes qui leur prêtent leurs services, des individus qui prêtent leurs services au gouvernement ou à l'institution ou à ces personnes ou organismes ou de ceux qui sont candidats à ces emplois ou désireux de prêter ces services;
- b) qu'exigent des administrations provinciales ou étrangères ou leurs organismes.

1980-81-82-83, ch. 111, ann. II « 23 ».

Individus
condamnés pour
une infraction

24. Le responsable d'une institution fédérale peut refuser à un individu la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui ont été recueillis ou obtenus par le Service correctionnel du Canada ou la Commission nationale des libérations conditionnelles pendant qu'il était sous le coup d'une condamnation à la suite d'une infraction à une loi fédérale, dans les cas où la communication risquerait vraisemblablement :

- a) soit d'avoir de graves conséquences sur son programme pénitentiaire, son programme de libération conditionnelle ou son programme de libération d'office;
- b) soit d'entraîner la divulgation de renseignements qui, à l'origine, ont été obtenus expressément ou implicitement à titre confidentiel.

L.R. (1985), ch. P-21, art. 24; 1994, ch. 26, art. 56.

Sécurité des
individus

25. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) dont la divulgation risquerait vraisemblablement de nuire à la sécurité des individus.

1980-81-82-83, ch. 111, ann. II « 25 ».

Renseignements
concernant un
autre individu

26. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui portent sur un autre individu que celui qui fait la demande et il est tenu de refuser cette communication dans les cas où elle est interdite en vertu de l'article 8.

1980-81-82-83, ch. 111, ann. II « 26 ».

Secret
professionnel des
avocats

27. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui sont protégés par le secret professionnel qui lie un avocat à son client.

1980-81-82-83, ch. 111, ann. II « 27 ».

Dossiers
médicaux

28. Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) qui portent sur l'état physique ou mental de l'individu qui en demande communication, dans les cas où la prise de connaissance par l'individu concerné des renseignements qui y figurent desservirait celui-ci.

1980-81-82-83, ch. 111, ann. II « 28 ».