Nations Unies ST/SGB/2004/15*

Secrétariat

29 novembre 2012

Circulaire du Secrétaire général

Utilisation des moyens et des données informatiques et télématiques**

Afin de définir les utilisations autorisées de l'informatique et des moyens et données connexes, et de garantir la sécurité et l'intégrité technique du système, le Secrétaire général promulgue ce qui suit :

Section 1
Définitions

Aux fins de la présente circulaire, on entend par :

a) *Utilisateur autorisé* : tout fonctionnaire autorisé à utiliser des moyens informatiques ou télématiques;

b) *Moyen informatique ou télématique* : tout bien corporel ou incorporel capable de produire, d'acheminer, de recevoir, de traiter ou de représenter des données numérisées, ledit bien pouvant appartenir à l'Organisation, ou être exploité sous licence ou selon d'autres modalités ou être géré, mis à disposition ou utilisé autrement par elle;

c) *Données informatiques ou télématiques* : toutes données ou informations, quels qu'en soient la forme et le support, qui sont ou ont été produites, acheminées, reçues, traitées ou représentées par des moyens informatiques ou télématiques;

d) *Utilisation pour les besoins du service* : utilisation de moyens informatiques ou télématiques par tout utilisateur autorisé dans l'exercice de ses fonctions et dans les limites de l'autorisation dont il bénéficie;

* Nouveau tirage pour raisons techniques (7 novembre 2012).

** On trouvera dans l'annexe à la présente circulaire des commentaires sur certaines de ses dispositions, qui, textes administratifs et exemples à l'appui, viennent les expliciter en les replaçant dans leur contexte. Ne faisant pas partie de la circulaire proprement dite, les commentaires n'ont valeur ni de règle de droit ni de texte réglementaire. Ils se veulent néanmoins un guide officiel (publié par l'Organisation) à l'usage de l'Administration et des fonctionnaires, qui renseignent sur la portée et les modalités d'application des dispositions en question. Les fonctionnaires visés par la circulaire peuvent donc se guider sur ces commentaires, dont l'Administration s'inspire pour interpréter et appliquer les dispositions en question. Les commentaires seront mis à jour à l'usage, en consultation avec les représentants du personnel siégeant au Comité de coordination entre l'Administration et le personnel institué par le chapitre VIII du Règlement du personnel.

04-62595* (F) 211112 231112

e) *Utilisation à des fins personnelles ou utilisation personnelle* : utilisation de moyens informatiques ou télématiques par tout utilisateur autorisé à des fins autres que les besoins du service;

f) *Données d'accès restreint* : données informatiques ou télématiques classifées ou dont l'utilisation ou la distribution est restreinte par un texte administratif.

Section 2
Conditions d'utilisation de données ou moyens informatiques ou télématiques

a) Les données et moyens informatiques ou télématiques doivent en toute circonstance être utilisés conformément aux dispositions de la présente circulaire et à celles des autres textes administratifs applicables;

b) Tout utilisateur autorisé qui a connaissance d'une infraction aux dispositions de la présente circulaire doit la dénoncer sans tarder à l'autorité compétente au sein de l'Organisation.

Section 3
Utilisation pour les besoins du service

3.1 Tout utilisateur autorisé doit veiller à ce que l'utilisation qu'il fait des moyens et données informatiques et télématiques soit conforme aux obligations attachées à sa qualité de fonctionnaire ou à toute autre obligation dont il serait tenu.

3.2 Tout utilisateur autorisé s'emploie :

a) À garantir l'exactitude de toutes données dont il est responsable;

b) À préserver et protéger les moyens et données informatiques et télématiques dont l'Organisation pourrait avoir besoin à une fin quelconque.

3.3 L'accès aux données d'accès restreint, la possession de telles données et leur distribution doivent obéir aux règles, règlements et textes administratifs applicables.

Section 4
Utilisation personnelle limitée

4.1 Il est loisible à tout utilisateur autorisé de se servir des moyens informatiques et télématiques à des fins personnelles, de façon limitée, à condition :

a) Que cette utilisation ne soit pas contraire aux normes de conduite les plus strictes, attachées à la qualité de fonctionnaire international (sont manifestement exclus l'acquisition ou la distribution de produits pornographiques, la pratique du jeu ou le déchargement de fichiers audio ou vidéo auxquels l'utilisateur n'a pas légalement accès);

b) Qu'il n'y ait aucune raison de craindre que cette utilisation nuise aux intérêts de l'Organisation ou à sa réputation;

c) Que cette utilisation ne soit pas onéreuse pour l'Organisation;

d) Que le fonctionnaire se livre à cette utilisation en dehors des heures de travail, ou que celle-ci n'enlève guère à son temps de travail;

e) Que cette utilisation ne diminue en rien l'aptitude de l'utilisateur autorisé ou de ses collègues à exercer leurs fonctions;

f) Que cette utilisation ne perturbe pas les activités ou le fonctionnement de l'Organisation et ne nuise en rien à l'efficacité des moyens informatiques et télématiques.

4.2 Lorsqu'il se sert des moyens informatiques et télématiques à des fins personnelles, tout utilisateur autorisé veille à ce que la nature privée et non professionnelle de cette utilisation soit manifeste.

4.3 L'utilisation à des fins personnelles est un privilège qui peut être modifié ou retiré à tout moment, selon qu'il convient à l'Organisation. Tout utilisateur autorisé assume l'entière responsabilité des conséquences de cette utilisation, ainsi que toute obligation financière qui pourrait en résulter, l'Organisation n'encourant aucune responsabilité ni aucune obligation en la matière.

Section 5
Activités interdites

5.1 Sont interdits à tout utilisateur autorisé de moyens ou données informatiques ou télématiques :

a) Le fait, sciemment ou par suite de faute lourde, de créer des données informatiques ou télématiques fausses ou propres à induire en erreur;

b) Le fait, sciemment ou par suite de faute lourde, de permettre à des personnes non autorisées de se servir de moyens ou données informatiques ou télématiques;

c) Le fait, sciemment ou par suite de faute lourde, d'utiliser des moyens ou données informatiques ou télématiques d'une manière contraire aux droits et obligations attachés à sa qualité de fonctionnaire;

d) Le fait, sciemment et sans justification ni autorisation ou par suite de faute lourde, d'abîmer, d'endommager, d'effacer, d'altérer, de détourner de leur finalité, de dissimuler ou de faire disparaître les données informatiques ou télématiques, y compris le fait de brancher des moyens informatiques ou télématiques étrangers à l'Organisation sur ceux de l'Organisation ou de stocker des données étrangères parmi celles de l'Organisation;

e) Le fait de consulter des données informatiques ou télématiques, sachant qu'il n'y est pas autorisé ou de se servir, sachant qu'il n'y est pas autorisé, de tout ou partie d'un moyen informatique ou télématique, y compris les transmissions électromagnétiques;

f) Le fait, sciemment ou par suite de faute lourde, de se servir des moyens ou données informatiques ou télématiques d'une manière qui enfreint un contrat liant l'Organisation ou un contrat de licence portant sur lesdits moyens ou lesdites données ou qui est contraire à la législation internationale sur les droits d'auteur;

g) Le fait, sciemment ou par suite de faute lourde, de tenter de se livrer à l'une quelconque des activités interdites dans la présente section, ou d'aider un tiers à s'y livrer.

Section 6
Droits afférents aux moyens informatiques et télématiques et protection de l'intégrité technique et du bon fonctionnement de ces moyens

6.1 a) L'Organisation se réserve tous les droits afférents aux moyens et aux données informatiques et télématiques et à tout produit du travail effectué par tout utilisateur autorisé au moyen desdits moyens ou données;

b) L'Organisation a le droit de couper ou de restreindre, à tout moment et sans préavis, l'accès à n'importe quels moyens ou données informatiques ou télématiques, lorsque c'est nécessaire pour préserver ou rétablir l'intégrité technique ou le bon fonctionnement desdits moyens ou données ou pour tout autre motif, y compris pour empêcher toute activité interdite visée à la section 5 de la présente circulaire.

Section 7
Contrôles et investigations

7.1 Toute utilisation des moyens ou données informatiques ou télématiques est soumise à contrôles et investigations ainsi qu'il est prévu aux sections 8 et 9 ci-après.

7.2 Les contrôles et investigations sont effectués par la Division de l'informatique, par ses homologues désignés par le Département de la gestion dans les bureaux hors Siège ou par le Bureau des services de contrôle interne (BSCI), ainsi qu'il est indiqué aux sections 8 et 9 ci-après.

7.3 Les fonctionnaires autorisés à contrôler l'utilisation des moyens informatiques et télématiques ou à enquêter sur ce sujet ont accès à tous moyens et données utiles, y compris les fichiers de données et de traitement de texte, les messages électroniques, les données enregistrées concernant le réseau local et l'accès à Internet et à l'intranet, le matériel informatique et les logiciels, l'information concernant les services téléphoniques et toutes autres données accessibles aux utilisateurs ou créées par eux.

Section 8
Contrôles et investigations effectués par la Division de l'informatique ou ses homologues hors Siège

8.1 Le suivi technique de l'utilisation des moyens informatiques et télématiques est assuré systématiquement aux fins du dépannage, de l'établissement de diagnostics, de l'analyse statistique et du réglage du fonctionnement desdits moyens, ce qui peut donner lieu à la production de données globales aux fins du suivi général de leur utilisation.

8.2 Dès lors qu'il y a des raisons de penser que les moyens informatiques et télématiques ont fait l'objet de quelque utilisation qui en perturbe le fonctionnement ou crée des problèmes techniques, la Division de l'informatique ou un de ses homologues hors Siège peut procéder à un contrôle ou à une investigation.

8.3 La Division de l'informatique ou son homologue hors Siège enquête à la demande soit du fonctionnaire habilité à ouvrir l'investigation en vertu de l'instruction administrative ST/AI/371, soit du BSCI.

8.4 a) Sauf le cas visé au paragraphe 9.1 ci-après, les demandes d'investigation concernant l'utilisation des moyens informatiques et télématiques sont adressées au Secrétaire général adjoint à la gestion ou, dans les bureaux hors Siège, au chef des services administratifs. Faites par écrit, elles décrivent brièvement les informations recherchées, le nom du fonctionnaire ou de la personne en cause et le nom du fonctionnaire habilité à recevoir les informations au sein du bureau demandeur;

b) À titre exceptionnel, l'investigation peut être ouverte à la demande faite oralement par tout fonctionnaire habilité du bureau demandeur, étant entendu qu'une demande écrite suivra dans les meilleurs délais;

c) L'investigation ne commence qu'après que la demande a été approuvée par le Secrétaire général adjoint à la gestion ou, dans un bureau hors Siège, par le chef des services administratifs;

d) Hors les cas d'urgence, le Secrétaire général adjoint à la gestion ou, dans un bureau hors Siège, le chef des services administratifs consulte le directeur de la Division des investigations du BSCI avant d'accéder à la demande d'investigation, afin de s'assurer que celle-ci n'empiète pas sur le mandat et les attributions du Bureau.

8.5 En cas d'investigation, il sera procédé comme suit :

a) Le fonctionnaire en cause et son supérieur hiérarchique sont informés par le bureau chargé de l'investigation juste avant l'examen de leurs moyens ou données informatiques ou télématiques, y compris les fichiers électroniques, le courrier électronique et les données sur l'accès à Internet et à l'intranet;

b) i) Chaque fois que possible, les contrôles matériels portant sur les moyens ou données informatiques ou télématiques sont effectués en présence de l'intéressé, de son supérieur hiérarchique et d'un représentant du bureau intéressé;

ii) Si l'intégrité de l'investigation le commande, l'accès aux moyens ou données informatiques ou télématiques qui en font l'objet, y compris les ordinateurs, fichiers électroniques et services de messagerie électronique, peut être interdit au fonctionnaire;

c) Le fonctionnaire habilité du bureau intéressé signe, le cas échéant, un reçu accusant réception de toutes informations;

d) Un dossier spécial est tenu en lieu sûr à la Division de l'informatique ou dans le bureau hors Siège chargé de l'investigation, dossier dans lequel sont consignés un bref énoncé de la demande d'investigation, le nom du demandeur, le compte rendu des actes accomplis à l'occasion de l'investigation, le nom des fonctionnaires qui y ont procédé et le type d'information trouvé et remis au demandeur;

e) Les informations trouvées et remises au demandeur ne restent pas en la possession de la Division de l'informatique ou du bureau hors Siège. L'original de la demande écrite et signée et les reçus relatifs à toutes informations communiquées au bureau intéressé sont conservés dans un dossier distinct tenu en lieu sûr au Bureau du Secrétaire général adjoint à la gestion ou dans le bureau hors Siège;

f) Les contrôles et investigations ne durent que le temps raisonnablement nécessaire pour déterminer si les faits reprochés au fonctionnaire sont constants. S'il

n'y a pas lieu à suivre, le fonctionnaire en est informé par le bureau qui a demandé les contrôles ou l'investigation, ainsi qu'il est prévu dans l'instruction administrative ST/AI/371.

Section 9
Investigations menées par le BSCI

9.1 De par son mandat, le BSCI dans l'exercice de ses attributions, s'agissant notamment d'ouvrir des enquêtes et investigations, agit d'office et en toute indépendance.

9.2 Les dispositions suivantes régissent les investigations du BSCI concernant des moyens ou données informatiques :

a) En cas d'impossibilité pratique, les demandes du BSCI d'accès à tous moyens ou données informatiques ou télématiques peuvent ne pas être présentées par écrit ni à l'avance;

b) Le BSCI est habilité à examiner les moyens ou données informatiques ou télématiques à distance, sans en informer le fonctionnaire;

c) Si possible, il est procédé à l'intervention matérielle sur des moyens situés au poste de travail du fonctionnaire en cause en sa présence, ou en présence du chef de sa division, de sa section ou de son groupe;

d) Le BSCI tient par écrit un relevé des interventions concernant tous moyens ou données informatiques ou télématiques, qui comporte une brève description des actes accomplis à l'occasion de l'investigation, le nom des personnes qui y ont procédé et le type d'information trouvé, aucune autre pièce relative à ces actes n'étant conservée dans aucun autre service;

e) La Division de l'informatique ou le bureau hors Siège désigne nommément des personnes, à savoir un fonctionnaire et au maximum deux suppléants, chargées de fournir au BSCI, à sa demande et selon qu'il juge nécessaire ou opportun, toute aide nécessaire pour avoir accès à tous moyens ou données informatiques ou télématiques. Différents fonctionnaires de la Division peuvent être désignés pour différentes catégories de moyens informatiques ou télématiques.

Section 10
Disposition finale

La présente circulaire entre en vigueur le 1er décembre 2004.

Le Secrétaire général
(*Signé*) Kofi A. **Annan**

Annexe à la circulaire du Secrétaire général

Commentaires

A. Section 1

1. On trouvera ici la définition des principaux termes utilisés dans la circulaire.

2. La définition a) s'applique à tous les fonctionnaires qui sont autorisés à utiliser des moyens informatiques ou télématiques. En sont exclus ceux qui bénéficient de la même autorisation tout en appartenant à une des catégories suivantes : sous-traitants, consultants, personnel fourni à titre gracieux, stagiaires non rémunérés, certains non fonctionnaires au service de l'Organisation et autres personnes ayant des liens avec l'Organisation sans en être fonctionnaires. Aussi convient-il de veiller à voir préciser dans les contrats ou autres pièces régissant la nomination de ces personnes ou entités que les dispositions de la présente circulaire s'appliquent à elles, *mutatis mutandis*, et ce, soit en par envoi à la présente circulaire soit par d'autres moyens appropriés.

L'autorisation visée dans cette définition et ailleurs dans la circulaire, sauf à l'alinéa e) du paragraphe 4.1, est celle dont on peut raisonnablement déduire qu'elle est accordée au fonctionnaire du fait des responsabilités attachées à ses fonctions ou en vertu d'instructions données par un supérieur hiérarchique à ce habilité.

3. La définition b) englobe tout le matériel et tous les logiciels capables de traiter ou de stocker des données. Elle comprend donc le matériel informatique (ordinateurs de bureau ou portables, serveurs, imprimantes, etc.), les logiciels (systèmes d'exploitation, applications destinées à augmenter la productivité, systèmes de gestion de base de données, etc.), les réseaux informatiques (supports matériels, matériel de commutation, pare-feu, équipement pour transmissions sans fil, etc.), le matériel, les logiciels et les réseaux téléphoniques (autocommutateurs privés, téléphones portables, etc.), les systèmes de sonorisation et d'enregistrement des votes, les installations de radiotélévision, les agendas électroniques, y compris ceux qui donnent accès sans fil à Internet et à la messagerie électronique, le matériel de sécurité (détecteurs, caméras, signaux d'alarme, portes à accès électronique, etc.) et le matériel immobilier contrôlé par des moyens électroniques (ascenseurs, groupes électrogènes, systèmes de chauffage, de ventilation et de climatisation).

4. Se voulant générale, la définition c) englobe toutes les données et informations créées ou reçues par l'ONU, quelles que soient leur origine ou la forme qu'elles prendraient (conversations téléphoniques, par exemple, journal des communications, information provenant des fichiers de courrier électronique et de traitement de texte, du SIG, de télécopies ou d'autre source électronique et utilisée dans une note écrite ou sur un autre support non électronique).

5. L'expression « besoins du service » [définition d)] englobe les activités dont on peut dire raisonnablement qu'elles intéressent la représentation du personnel, par exemple l'organisation de réunions, les campagnes électorales pour les élections syndicales, les travaux des comités, associations et organes paritaires et l'examen des questions intéressant les représentants du personnel.

6. L'autorisation visée par la définition e) est celle envisagée à la section 4 de la présente circulaire.

7. De la combinaison de la définition de l'» utilisateur autorisé » et des définitions d) et e) de la section 1 il résulte quatre catégories de personnes : i) les utilisateurs qui ne sont pas des utilisateurs autorisés; ii) les utilisateurs autorisés agissant pour les besoins du service; iii) les utilisateurs autorisés agissant à des fins personnelles; iv) les utilisateurs autorisés qui agissant à des fins qui débordent le champ de leur autorisation.

8. La définition f) vise les données informatiques ou télématiques qui, pour des raisons de sécurité, de sûreté, de protection de la vie privée, de confidentialité ou autres, sont classifiées ou méritent des précautions particulières et doivent être désignées comme telles, conformément aux textes administratifs en vigueur ou à venir. La circulaire ST/SGB/272 et les instructions administratives ST/AI/326 et ST/AI/189/Add.16 renseignent sur toutes informations classifiées ou dont la distribution est restreinte.

B. Section 2

1. À l'alinéa a), les autres textes administratifs applicables aux moyens et données informatiques et télématiques sont notamment ceux cités ci-dessus à propos de la définition des « données d'accès restreint ».

2. L'alinéa b) fait à tout fonctionnaire obligation de dénoncer toute infraction à la circulaire dont il aurait connaissance, même lorsque l'infraction concerne des moyens qu'il n'est pas autorisé à utiliser ou des données qu'il n'est pas autorisé à consulter. Cette obligation s'inscrit dans la même logique que celles résultant d'autres textes administratifs, par exemple la circulaire ST/SGB/2003/13 relative à la prévention de l'exploitation et de la violence sexuelles. Cela dit, cette disposition vise les seules infractions dont le fonctionnaire a connaissance dans l'exercice normal de ses activités. Comme il est dit à l'alinéa c) du paragraphe 5.1 de la circulaire, le fonctionnaire n'a pas le droit sans qualité d'enquêter sur l'utilisation que font ses collègues des moyens ou données informatiques ou télématiques. L'autorité onusienne à laquelle il convient de dénoncer les infractions varie selon la situation; ce peut être par exemple un supérieur hiérarchique, un chef de service ou le BSCI.

C. Section 3

1. Les utilisateurs autorisés sont engagés à se servir le plus possible des moyens et données informatiques et télématiques, dans les limites autorisées, et dans le but d'exécuter les tâches qui leur sont confiées aussi efficacement et économiquement que possible.

2. Selon le paragraphe 3.1 tout utilisateur autorisé doit veiller à ce que l'utilisation qu'il fait des moyens et données informatiques et télématiques soit conforme à toutes les autres obligations qui lui incombent en la matière. Dans le cas du fonctionnaire, il s'agit notamment des obligations résultant du Statut et du Règlement du personnel et de la circulaire intitulée « Statut et droits et devoirs essentiels des fonctionnaires de l'Organisation des Nations Unies » (ST/SGB/2002/13).

3. Paragraphe 3.2 : tout utilisateur autorisé a notamment pour obligation de veiller à ce que les données informatiques et télématiques puissent être consultées par tous les autres utilisateurs autorisés qui en ont besoin dans l'exercice de leurs fonctions. L'obligation de préserver et protéger autant que possible les moyens et données informatiques et télématiques s'impose spécialement dès lors que ces moyens ou données sont nécessaires aux fins de telles ou telles investigations.

D. Section 4

1. Il résulte de cette section que le fonctionnaire a le droit de se servir de temps à autre des moyens informatiques et télématiques de l'Organisation à des fins personnelles, et ce, dans certaines limites et sous certaines conditions.

2. Il ressort de l'alinéa a) du paragraphe 4.1 dispose que l'utilisation personnelle à laquelle se livre tout utilisateur autorisé doit être conforme aux normes de conduite les plus strictes attachées à la qualité de fonctionnaire international. On trouvera des précisions sur ces normes dans le Règlement du personnel et dans la circulaire susmentionnée (ST/SGB/2002/13).

3. À l'alinéa c) du paragraphe 4.1, ce qui « n'est pas onéreux pour l'Organisation » peut désigner par exemple la consommation de papier, d'encre, de toner, etc., l'usure du matériel ou des frais de télécommunication négligeables.

4. En ce qui concerne le paragraphe 4.2, il arrive que la nature de l'utilisation ou le contexte dans lequel elle s'inscrit ne laissent subsister aucun doute sur sa nature privée et non professionnelle. Dans les cas où sa nature n'est pas manifeste, on peut l'indiquer, dans le cas du courrier électronique ou autre, par la mention « Cette correspondance est privée et n'a aucun caractère officiel ». Le Département de la gestion peut, après avis du Bureau des affaires juridiques, autoriser l'utilisation d'autres formules. Tout fonctionnaire prendra soin de dissocier sa correspondance privée de toute correspondance à caractère officiel.

5. À propos du paragraphe 4.3, il faut savoir que l'utilisation des moyens informatiques et télématiques à des fins personnelles, notamment pour la correspondance privée, n'est pas couverte par les privilèges et immunités des Nations Unies, et que l'Organisation concourt à l'action des autorités de police lorsqu'elles s'intéressent à toute utilisation personnelle interdite.

E. Section 5

1. Cette section énumère les activités interdites aux utilisateurs de moyens ou données informatiques ou télématiques. On se reportera aussi au paragraphe 2 du commentaire relatif à la section 4 sur ce sujet.

2. Exemples d'activités interdites à l'alinéa a) du paragraphe 5.1 : faux, falsification d'information, contrefaçon de signature électronique.

3. Exemple d'activité interdite à l'alinéa b) du paragraphe 5.1 : sciemment ou par suite d'une faute lourde, révéler des mots de passe permettant à des personnes qui n'y sont pas autorisées d'utiliser des moyens ou de consulter des données informatiques ou télématiques de l'Organisation, ou leur permettre de les utiliser par d'autres moyens.

4. Les droits et obligations du fonctionnaire visés à l'alinéa c) du paragraphe 5.1 sont notamment ceux qu'il tire du Règlement du personnel et de la circulaire susmentionnée (ST/SGB/2002/13).

5. Exemple d'activité interdite à l'alinéa e) du paragraphe 5.1 : rechercher systématiquement et sans autorisation dans les moyens informatiques et télématiques des failles qui les vulnérabilisent, notamment sur le plan de la sûreté.

6. Exemples d'activités interdites à l'alinéa f) du paragraphe 5.1 : sciemment ou par suite d'une faute lourde, se servir de logiciels piratés, télécharger des fichiers audio ou vidéo auxquels on n'a pas légalement accès, ou utiliser un logiciel dont l'utilisation n'est pas autorisée par accord de licence.

F. Sections 7, 8 et 9

1. Les sections 7, 8 et 9, qui traitent des contrôles et investigations concernant les moyens et données informatiques et télématiques, partent du principe que lesdits moyens et données appartiennent à l'Organisation et sont censés être utilisés pour les besoins du service, et que toute utilisation qu'en fait le fonctionnaire est assujettie aux droits de l'Organisation, y compris celui d'y accéder sans que le fonctionnaire le sache ou y ait consenti.

2. Les sections 8 et 9 définissent deux types de contrôles et d'investigations relatifs aux moyens et données informatiques et télématiques, selon qu'ils sont entrepris, d'une part, par la Division de l'informatique ou pour le compte d'un service de l'Organisation autre que le BSCI ou, de l'autre, par le BSCI.

3. Sont énoncées à la section 8 les règles applicables à tous les contrôles et à toutes les investigations hormis ceux effectués par le BSCI conformément à la section 9.

4. Le paragraphe 7.2 énumère les services habilités à effectuer des contrôles ou investigations concernant les moyens et données informatiques et télématiques, ou à y concourir.

5. La section 8 traite des contrôles et investigations effectués par la Division de l'informatique d'office ou pour le compte d'autres services. La Division et ses homologues hors Siège peuvent décider de procéder à des contrôles ou investigations en cas d'ingérence ou de perturbation technique touchant les moyens et données informatiques et télématiques. Ils peuvent aussi aider d'autres services à mener des investigations autorisées comme prévu par la circulaire ST/AI/371. Il est ouvert une investigation notamment lorsque le bureau demandeur estime qu'il y a lieu de penser qu'une faute professionnelle, éventuellement une infraction à la présente circulaire, a été commise. Toutes les investigations nécessitant l'accès aux moyens ou données informatiques ou télématiques ouvertes en vertu de la section 8 (hormis le paragraphe 8.2) doivent recevoir l'accord préalable du Secrétaire général adjoint à la gestion ou du chef des services administratifs dans les bureaux hors Siège. S'il est difficile de déterminer qui doit être considéré comme étant le chef des services administratifs, on demandera l'approbation du fonctionnaire de plus haut rang parmi ceux qui sont chargés de gérer les moyens informatiques et télématiques du lieu d'affectation considéré.

6. Le paragraphe 8.5 énonce les règles spéciales qui jouent en matière de contrôles et investigations de l'utilisation faite par tel ou tel fonctionnaire des moyens et données informatiques et télématiques, ainsi que plusieurs droits reconnus au fonctionnaire soumis à contrôle ou investigation, y compris celui d'être prévenu à l'avance que les moyens ou données informatiques ou télématiques dont il se sert vont être inspectés.

G. Section 9

1. Cette section est consacrée aux règles régissant les investigations du BSCI concernant des moyens ou données informatiques ou télématiques. Au regard de l'autorité dont le Bureau est investi, le fonctionnaire ne bénéficie pas des mêmes droits que ceux énoncés à la section 8 en matière de notification. Les investigations en question doivent être menées dans le respect des règles et des droits que le fonctionnaire tient de tous les textes applicables aux investigations du Bureau, y compris la résolution 48/218 B de l'Assemblée générale, de la circulaire ST/SGB/273 et du manuel de la Division des investigations du Bureau.

2. Il ressort du paragraphe 9.2 qu'une des règles gouvernant la matière est que le Bureau n'est tenu ni de déposer à l'avance une demande d'accès aux moyens ou données informatiques ou télématiques ni d'obtenir l'accord de quelque fonctionnaire qui lui soit extérieur. Selon l'alinéa c), le BSCI peut examiner à distance les moyens et données informatiques et télématiques d'un fonctionnaire, sans l'en informer. On notera en particulier que lorsque le Bureau inspecte des moyens situés au poste de travail de l'intéressé, il doit, si possible, le faire en présence de celui-ci ou de son chef de division, de section ou de groupe.