



# **Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail**

**A l'intention de l'administration fédérale**

État: octobre 2013



## Table des matières

<b>Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail</b> .....	<b>1</b>
A l'intention de l'administration fédérale.....	1
<b>Table des matières</b> .....	<b>2</b>
<b>1. Introduction: La surveillance de l'utilisation d'Internet et du courrier électronique</b> .....	<b>3</b>
<b>2. Intérêts concernés de l'employeur</b> .....	<b>3</b>
<b>3. Les données secondaires</b> .....	<b>4</b>
<b>4. Bases légales de la surveillance</b> .....	<b>4</b>
4.1 Proportionnalité .....	5
4.2 Finalité du traitement.....	5
4.3 Transparence .....	5
<b>5. Interdiction de la surveillance du comportement</b> .....	<b>5</b>
<b>6. Programmes de surveillance</b> .....	<b>6</b>
<b>7. Mesures techniques et organisationnelles de protection</b> .....	<b>6</b>
7.1 Mesures techniques .....	6
7.2 Mesures organisationnelles: le règlement d'utilisation .....	7
<b>8. Enregistrement des données secondaires</b> .....	<b>8</b>
<b>9. Utilisation abusive</b> .....	<b>8</b>
<b>10. Formes d'analyse</b> .....	<b>8</b>
10.1 Analyses ne se rapportant pas aux personnes (anonymes): art. 57m LOGA, art. 8 de l'ordonnance sur les données secondaires.....	8
10.2 Analyses non nominales se rapportant aux personnes (pseudonymes): art. 57n LOGA, art. 9 de l'ordonnance sur les données secondaires .....	9
10.3 Analyses nominales se rapportant aux personnes: art. 57o LOGA, art. 10 et 11 de l'ordonnance sur les données secondaires.....	9
10.4 Qui procède à l'analyse?.....	9
<b>11. Conditions de l'analyse</b> .....	<b>10</b>
11.1 Analyses ne se rapportant pas aux personnes: art. 8 de l'ordonnance sur les données secondaires .....	10
11.2 Analyses non nominales se rapportant aux personnes: art. 9 de l'ordonnance sur les données secondaires .....	11
11.3 Analyse nominale se rapportant aux personnes: art. 10, 11, 12 et 13 de l'ordonnance sur les données secondaires .....	11
11.3.1 Mandats d'analyse nominale se rapportant aux personnes en cas d'utilisation abusive ou de soupçon d'utilisation abusive: art. 10 de l'ordonnance sur les données secondaires .....	11
11.3.2 Déroulement des analyses nominales se rapportant aux personnes en cas d'utilisation abusive ou de soupçon d'utilisation abusive: art. 11 de l'ordonnance sur les données secondaires.....	12
11.3.3 Analyses nominales se rapportant aux personnes en vue d'éliminer des perturbations (et de parer à une menace concrète).....	13
11.3.4 Information sur les résultats des analyses.....	13



## 1. Introduction: La surveillance de l'utilisation d'Internet et du courrier électronique

Le présent guide explique d'une part aux employés de la Confédération selon quelles modalités et dans quel but leur utilisation d'Internet et du courrier électronique peut être surveillée, et il explique d'autre part aux organes fédéraux désirant surveiller l'utilisation que font leurs employés d'Internet et du courrier électronique quelles dispositions légales ils doivent ce faisant respecter. Seront notamment abordées les nouvelles dispositions de la loi sur l'organisation du gouvernement et de l'administration (LOGA), entrées en vigueur le 1er avril 2012, et la nouvelle ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442). Comme cette dernière ne dispose pas d'une abréviation officielle, elle sera appelée ci-après «ordonnance sur les données secondaires».

Rappelons pour commencer que l'administration fédérale n'avait pas, avant le 1er avril 2012, de dispositions réglant l'enregistrement ou l'analyse des données secondaires générées lors de l'utilisation d'Internet et du courrier électronique. Les dispositions en la matière des organes fédéraux appliquées avant le 1er avril 2012 n'avaient de ce fait aucune assise légale et doivent désormais être examinées quant à leur compatibilité avec les dispositions de la LOGA et de l'ordonnance sur les données secondaires.

Précisons encore que les nouvelles dispositions ne permettent qu'une surveillance a posteriori. Elles ne constituent pas une base légale pour la surveillance en temps réel (sur ce point, voir chif. 6, Programmes de surveillance) au moyen de programmes ou d'appareils prévus à cet effet (enregistreurs de frappes).

## 2. Intérêts concernés de l'employeur

Quand les employés écrivent des courriers électroniques et naviguent dans Internet, ils peuvent porter atteinte à certains intérêts et équipements techniques de l'employeur, par exemple:

- à la capacité de stockage et à la bande passante du réseau (réduction de la capacité du flux de données), suite à une utilisation excessive d'Internet et du courrier électronique;
- à la sécurité des données et des applications (disponibilité, intégrité, confidentialité) par l'importation de virus, de vers, de chevaux de Troie ou l'installation de logiciels étrangers;
- au temps de travail et à d'autres intérêts financiers (pertes de productivité, augmentation des coûts pour des moyens supplémentaires);
- à d'autres intérêts de l'employeur protégés par la loi tels que sa réputation, ses secrets de fabrication ou d'affaires ou encore la protection des données.



### 3. Les données secondaires

L'utilisation d'Internet et du courrier électronique laisse, à divers endroits, des traces que l'on nomme «données secondaires». Les outils informatiques utilisés en commun (par ex. les serveurs) établissent en général des journaux des activités exécutées. Ils créent des fichiers journaux qui contiennent les données secondaires.

Lors de l'utilisation d'Internet et du courrier électronique, seules les données secondaires sont normalement enregistrées; elles permettent de savoir qui a fait quoi. A des fins de sauvegarde (backup), il est cependant permis d'enregistrer aussi les contenus des courriers électroniques.

Les journaux pertinents pour la surveillance des collaborateurs peuvent pour l'essentiel être créés à quatre endroits: sur le poste de travail de l'utilisateur, sur les serveurs Intranet, sur les équipements de connexion interréseaux (pare-feux ou routeurs) et sur les serveurs de la «zone démilitarisée» (voir plus bas).

Sur des serveurs Intranet tels que les serveurs de domaine, les journaux comprennent les données suivantes: le nom de l'utilisateur (qui), la date (quand), les actions exécutées (connexion et déconnexion), l'attribution dynamique d'adresses IP, la résolution des noms de domaine et le lancement d'une application (quoi).

Des pare-feux protègent souvent une zone dite «démilitarisée» (DMZ) entre Intranet et Internet qui héberge les serveurs joignables des deux mondes. Il s'agit dans la plupart des cas de serveurs de courrier électronique, de serveurs de fichiers publics et de serveurs web.

Les serveurs de courrier électronique créent des fichiers journaux qui contiennent entre autres l'heure d'envoi ou de réception du message, l'adresse de l'expéditeur, l'adresse du destinataire, le contenu du champ «Objet», le degré de priorité et la confidentialité du message. Il n'est pas exclu que les fichiers journaux contiennent d'autres informations (par ex. le nombre de fichiers attachés, la taille du message, la signature électronique, voire l'adresse IP).

### 4. Bases légales de la surveillance

Les dispositions de la loi sur la protection des données (LPD) s'appliquent en sus de celles de la LOGA et de l'ordonnance sur les données secondaires. L'analyse des fichiers journaux (données secondaires) ici exposée constitue un traitement de données personnelles au sens de l'art. 3, let. e, LPD quand les données secondaires ne sont pas anonymisées avant l'analyse. En vertu de l'art. 17, al. 1, LPD, les organes fédéraux ont uniquement le droit de traiter des données personnelles quand il existe une base légale à cet effet. Dans le cas présent, cette base se fonde sur les dispositions correspondantes de la LOGA et de l'ordonnance sur les données secondaires. D'autres dispositions du droit fédéral sont réservées en vertu de l'art. 57i LOGA. Lors du traitement de données personnelles, il faut en outre tenir compte des dispositions générales en matière de protection des données des art. 4 ss LPD. Celles-ci concernent notamment les principes de la proportionnalité, de la finalité du traitement et de la transparence. Avant de passer aux dispositions légales spéciales, nous voulons rappeler brièvement les principes susmentionnés de la protection des données.



## 4.1 Proportionnalité

L'art. 4, al. 2, LPD dit qu'un traitement de données doit être effectué conformément au principe de la proportionnalité. Dans le contexte de l'analyse des données secondaires, cela signifie qu'il est uniquement possible de procéder aux analyses indispensables pour la mise au jour d'abus, pour remédier à des pannes ou pour réagir face à des menaces concrètes. L'organe fédéral ou l'exploitant de l'infrastructure électronique doit en outre choisir la forme d'analyse qui porte le moins atteinte aux droits de la personnalité des collaborateurs.

## 4.2 Finalité du traitement

Le principe de la finalité du traitement (art. 4, al. 3, LPD) veut que les données secondaires soient traitées uniquement dans le but prévu par une loi. Si l'organe fédéral ou l'exploitant de l'infrastructure électronique analysent les fichiers journaux dans un but qui n'est pas prévu par une loi, ils enfreignent le principe de la finalité du traitement et, par conséquent, les dispositions de la LOGA et de la LPD.

## 4.3 Transparence

A la différence de l'économie privée, l'organe fédéral ou l'exploitant de l'infrastructure électronique peut attendre des employés de la Confédération qu'ils connaissent les dispositions légales régissant la surveillance. L'organe fédéral ne doit donc en principe pas édicter de règlement en la matière. Il doit par contre satisfaire au principe de la transparence (art. 4, al. 4, LPD) en édictant un règlement d'utilisation d'Internet et du courrier électronique. Ce règlement revêt une grande importance car il définit la notion d'utilisation abusive. La transparence est aussi garantie moyennant la publication des résultats de l'analyse.

# 5. Interdiction de la surveillance du comportement

L'art. 26, al. 1, de l'ordonnance 3 relative à la loi sur le travail (OLT 3) s'applique aussi au sein de l'administration fédérale. Il interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des collaborateurs à leur poste de travail. Cette disposition vise à protéger la santé. L'utilisation des systèmes de surveillance ou de contrôle à d'autres fins est autorisée à condition que lesdits systèmes soient configurés de manière à ne pas porter atteinte à la santé et à la liberté de mouvement des collaborateurs.

S'agissant de l'utilisation d'Internet et du courrier électronique au lieu de travail, cela signifie qu'il est interdit de procéder à l'analyse permanente des fichiers journaux nominaux des collaborateurs.

L'utilisation d'enregistreurs de frappes et d'autres programmes de surveillance qui enregistrent la moindre activité du collaborateur à son poste de travail est aussi interdite en l'absence d'une ordonnance judiciaire en vertu de l'art. 26, al. 1, OLT 3.

Il est aussi fait usage de «content scanners» qui examinent chaque courrier électronique envoyé et reçu en fonction de termes prédéfinis et qui réagissent en conséquence (en bloquant le courrier, en l'effaçant ou en envoyant une copie à l'administrateur système, voire au supérieur hiérarchique). L'utilité de ces programmes est sujette à controverse dans la mesure où les collaborateurs peuvent pour ainsi dire s'«accommoder» de ces programmes et les contourner en utilisant des signes spéciaux ou un langage



codé. Le traitement de chaque courrier électronique au moyen de content scanners soulève aussi la question de la surveillance du comportement, en principe interdite (voir aussi chif. 6).

## 6. Programmes de surveillance

Les nouvelles dispositions de la LOGA ne constituent pas une base légale suffisante pour l'utilisation de programmes de surveillance installés sur l'ordinateur du collaborateur. En raison des atteintes massives aux droits de la personnalité des collaborateurs qu'ils constituent, lesdits programmes peuvent uniquement être utilisés moyennant une ordonnance judiciaire.

Les programmes installés directement sur l'ordinateur rendent possible une surveillance poussée de l'ensemble des activités du collaborateur. Ils permettent de lire les contenus des courriers électroniques et génèrent à intervalles réguliers des captures d'écran. Les enregistreurs de frappe permettent de consigner tous les textes tapés sur le clavier. Comme les programmes de surveillance consignent de manière systématique les activités des collaborateurs, les utiliser en l'absence d'une ordonnance judiciaire revient à enfreindre l'interdiction de la surveillance du comportement (voir chif. 5).

## 7. Mesures techniques et organisationnelles de protection

Avant de procéder à la surveillance nominale d'un collaborateur, les organes fédéraux doivent aussi se demander quelles mesures techniques et organisationnelles ils ont déjà prises ou peuvent encore prendre pour empêcher des abus.

Les organes fédéraux doivent naturellement communiquer à leurs collaborateurs quelles utilisations du courrier électronique et d'Internet sont autorisées et lesquelles ne le sont pas. Chaque organe fédéral édictera à cet effet un règlement d'utilisation que les collaborateurs devront connaître. Ce règlement aura, avec les nouvelles dispositions, un rôle majeur puisque la notion d'utilisation abusive y sera définie comme une violation des dispositions en matière d'utilisation (voir chif. 9, Utilisation abusive).

### 7.1 Mesures techniques

L'authentification et l'autorisation, les applications de chiffrement, les logiciels antivirus, les gestionnaires de quotas disque, les backups et les pare-feux comptent parmi les principales mesures techniques. Les logiciels de courrier électronique et les navigateurs doivent bien évidemment être configurés dans le respect des avancées technologiques les plus récentes et être actualisés régulièrement.

S'agissant de l'**authentification**, il faudrait implémenter une solution à deux facteurs (mot de passe et par ex. carte à puce électronique). L'**autorisation** garantit que certaines données ne sont accessibles qu'aux personnes qui en ont effectivement besoin pour accomplir leurs tâches. A cette fin, on définira les rôles et les droits d'accès de chacun.

**Il faut utiliser des applications de chiffrement** pour garantir que des données personnelles ou des profils de la personnalité confidentiels ou particulièrement dignes de protection ne puissent être traités que par les personnes qui disposent de l'autorisation nécessaire. Parmi ces applications, mentionnons Secure Messaging, Secure Center et BitLocker.



**Les gestionnaires de quotas disque** sont des logiciels qui limitent l'espace disque dont peut disposer un utilisateur pour ses fichiers et courriers électroniques. Ils permettent d'éviter des surcharges inutiles de la capacité du disque.

**Les pare-feux** protègent les données contre les attaques extérieures et évitent que la bande passante et le temps de travail ne soient trop sollicités. Ils peuvent être complétés par une liste de sites interdits. Cette liste dite négative comprend les adresses des sites Internet sur lesquels les collaborateurs ne doivent pas pouvoir se rendre. Il est aussi possible d'établir une liste dite positive, qui comprend les adresses des sites auxquels les collaborateurs peuvent accéder.

Le téléchargement de fichiers peut être limité aux fichiers d'un **format particulier** (.exe, .mp3, .bat), mais cette mesure n'a que des effets limités puisque des fichiers d'archives comprimés (.zip) peuvent contenir des fichiers ayant un format bloqué.

## 7.2 Mesures organisationnelles: le règlement d'utilisation

L'édictation d'un règlement d'utilisation d'Internet et du courrier électronique constitue la principale mesure organisationnelle. Les organes fédéraux définissent, dans ce règlement, la manière dont les collaborateurs peuvent utiliser Internet et le courrier électronique à titre professionnel et à titre privé. Les nouvelles dispositions de la LOGA accordent une place centrale au règlement d'utilisation puisque les organes fédéraux y définissent aussi quels comportements sont à considérer comme abusifs.

Le règlement d'utilisation (voir annexe) assure la transparence et la sécurité du droit. Il évite ainsi des discussions superflues entre les organes fédéraux et les collaborateurs. Le règlement doit être porté à la connaissance du personnel; cela se fera en général par écrit. A des fins de preuve, les organes fédéraux demanderont aux collaborateurs de confirmer qu'ils ont bien reçu le règlement. Les services de grande taille portent généralement le règlement à la connaissance de leurs collaborateurs par voie électronique. Les collaborateurs reçoivent alors souvent un courrier électronique contenant le lien qui mène au règlement d'utilisation, consultable dans le domaine Intranet de l'organe fédéral. Il est permis de procéder aussi de cette manière. L'organe fédéral doit informer le personnel de toute modification du règlement.

Un règlement d'utilisation peut être édicté pour un département entier et s'appliquer ainsi à tous les collaborateurs. Mais les offices fédéraux ou les différents services édictent souvent leurs propres règlements. Cela fait en particulier sens quand les collaborateurs doivent, pour l'accomplissement de leur travail, utiliser Internet et le courrier électronique d'une manière qui diverge de l'utilisation autorisée dans le reste du département. Le principe suivant s'applique: les collaborateurs doivent se tenir au règlement qui a été porté à leur connaissance (principe de la transparence).

L'organe fédéral permet normalement au personnel d'utiliser Internet et le courrier électronique à titre privé dans certaines limites. Il est ainsi possible de naviguer dans Internet tant que cela ne nuit pas à l'accomplissement des obligations contractuelles. En fonction du champ d'activité, il peut être indiqué d'interdire complètement l'utilisation d'Internet et du courrier électronique à titre privé. L'organe fédéral qui ordonne une telle interdiction totale doit cependant savoir qu'appliquer cette interdiction et en contrôler le respect demande beaucoup de temps et d'efforts.

On peut dire en résumé que plus le règlement d'utilisation est clair, mieux le personnel sait ce qui est permis et ce qui est interdit. On évite ainsi les conflits inutiles.



## 8. Enregistrement des données secondaires

L'art. 57/LOGA règle dans quels buts les données secondaires et les contenus des courriers électroniques peuvent être enregistrés. Les organes fédéraux ne peuvent cependant enregistrer le contenu des courriers électroniques qu'à des fins de sauvegarde (backup); il n'est donc pas accessible dans le cadre de la surveillance de l'utilisation.

Les données secondaires générées lors de l'utilisation d'Internet et du courrier électronique peuvent, en vertu de l'art. 57I, let. b, LOGA, être enregistrées à différentes fins. Seuls les chif. 1, 2 et 3 de ladite disposition sont ici pertinents. Les buts autorisés sont:

- le maintien de la sécurité de l'information et des services;
- l'entretien technique de l'infrastructure électronique;
- le contrôle du respect des règlements d'utilisation.

## 9. Utilisation abusive

L'art. 10, al. 1, de l'ordonnance sur les données secondaires définit la notion d'utilisation abusive. Il y a abus lorsque l'utilisation de l'infrastructure électronique enfreint les prescriptions de l'organe fédéral ou de la législation par sa nature, son ampleur ou sa fréquence. L'importance de l'édiction, par l'organe fédéral, de dispositions concernant l'utilisation sous la forme de règlements d'utilisation est patente dans ces cas. En l'absence d'un tel règlement, l'organe fédéral peut uniquement faire valoir l'infraction contre les dispositions légales comme abus et, ainsi, comme motif d'une analyse nominale des données.

On peut en principe distinguer les deux formes d'abus suivantes:

1. **Abus en termes quantitatifs:** Le collaborateur utilise plus que de raison Internet et le courrier électronique à titre privé. Il abuse des ressources et des moyens de l'organe fédéral.
2. **Abus en termes qualitatifs:** Le collaborateur consulte des sites Internet aux contenus illégaux ou définis comme illicites par l'organe fédéral. Le harcèlement par courrier électronique relève aussi de l'abus en termes qualitatifs.

## 10. Formes d'analyse

L'analyse des données secondaires peut prendre trois formes fondamentales. En vertu du principe de la proportionnalité, l'organe fédéral doit toujours choisir la forme qui est appropriée pour le but visé (l'empêchement ou la mise au jour d'abus) et constitue l'atteinte la moins importante aux droits de la personnalité de la personne concernée. Les trois formes sont décrites ci-dessous.

### 10.1 Analyses ne se rapportant pas aux personnes (anonymes): art. 57m LOGA, art. 8 de l'ordonnance sur les données secondaires

Les fichiers journaux sont nominaux puisqu'ils fournissent des informations sur les personnes qui les ont générés. Il peut s'agir de l'adresse de courrier électronique, de l'adresse IP ou d'un numéro d'identification du collaborateur. L'analyse anonyme des données secondaires n'implique pas que les données doivent être rendues anonymes avant l'analyse. Les résultats de l'analyse sont présentés sous



une forme purement statistique, sans rapport avec une personne particulière, et donc anonyme. L'analyse anonyme pourrait s'articuler comme suit: Combien de sites Internet à contenu pornographique sont consultés chaque mois par le personnel ? Les analyses anonymes peuvent être effectuées sans limite de temps ni de contenu pour tous les buts visés à l'art. 57l LOGA. Le but principal est de contrôler le respect des règlements d'autorisation (art. 57l, let. b, chif. 3, LOGA).

## **10.2 Analyses non nominales se rapportant aux personnes (pseudonymes): art. 57n LOGA, art. 9 de l'ordonnance sur les données secondaires**

Comme les fichiers journaux contiennent le nom du collaborateur (courrier électronique) ou une adresse IP/un numéro d'identification (Internet), ils peuvent permettre d'identifier la personne concernée. Dans le contexte d'une analyse non nominale se rapportant aux personnes, il faut utiliser des pseudonymes dans les résultats de l'analyse pour empêcher qu'un rapport puisse être établi avec les personnes concernées. Une telle analyse pourrait s'articuler comme suit: Y a-t-il, dans un service particulier, des collaborateurs qui envoient plus de 100 courriers électroniques par mois ? Le collaborateur qui remplit ce critère figurera dans la liste sous un pseudonyme. Cette forme d'analyse ne peut être effectuée que **par sondages (donc pas de manière systématique)** pour contrôler l'utilisation de l'infrastructure électronique (art. 57, let. b, LOGA). Il n'est donc pas indispensable qu'il y ait un soupçon d'abus pour y procéder.

## **10.3 Analyses nominales se rapportant aux personnes: art. 57o LOGA, art. 10 et 11 de l'ordonnance sur les données secondaires**

Ici, le résultat de l'analyse des données secondaires est présenté en rapport concret avec une ou plusieurs personnes. Cette analyse pourrait s'articuler comme suit: Quels collaborateurs utilisent Internet pendant plus de deux heures par jour ? Le résultat est présenté avec des informations qui permettent d'identifier la personne concernée (nom, numéro d'identification ou autres identifiants utilisés au sein de l'organe fédéral). L'analyse nominale se rapportant aux personnes est permise pour élucider un soupçon concret d'utilisation abusive de l'infrastructure électronique ou pour poursuivre un cas d'utilisation abusive (art. 57o, al. 1, let. a, LOGA). L'importance centrale du règlement d'utilisation, qui définit concrètement les utilisations abusives, est ici patente.

## **10.4 Qui procède à l'analyse?**

Nous définirons ici, pour commencer, quelques-unes des notions qui figurent dans les nouvelles dispositions de la LOGA et de l'ordonnance sur les données secondaires.

Les analyses peuvent en principe être effectuées ou ordonnées par:

- l'exploitant du système;
- le service prévu dans le concept de protection des données de l'organe fédéral, ou
- l'organe fédéral.

Afin que les développements relatifs aux conditions réglant les analyses soient clairs, il faut préciser les points suivants:

On entend par **exploitant du système** au sens de l'art. 1, let. c, de l'ordonnance sur les données secondaires le service chargé de la gestion technique de l'infrastructure électronique de la Confédération. En ce qui concerne Internet et le courrier électronique, il s'agit dans la plupart des cas de l'Office fédéral



de l'informatique et de la télécommunication (OFIT). Certains départements, par exemple le DDPS, exploitent cependant leur propre centre de calcul pour ces tâches.

Le **service prévu dans le concept de protection des données de l'organe fédéral** est en général le conseiller à la protection des données de l'organe fédéral.

On entend par **organes fédéraux** les autorités et les services de la Confédération (départements, offices, Chancellerie fédérale, unités administratives décentralisées, établissements fédéraux, etc.) ainsi que les personnes physiques et morales en dehors de l'administration fédérale, pour autant qu'elles soient chargées de tâches publiques de la Confédération (comme la Poste, les CFF et la SUVA).

On entend par **données administrées** au sens de l'art. 1, let. a, de l'ordonnance sur les données secondaires les données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de la Confédération et qui sont régulièrement utilisées, analysées ou effacées volontairement. Des données administrées (données secondaires) sont générées là où des appareils sont exploités en réseau.

On entend par **données non administrées** au sens de l'art. 1, let. b, de l'ordonnance sur les données secondaires les données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique de la Confédération mais qui ne sont pas ou qui ne sont pas régulièrement utilisées, analysées ou effacées volontairement. Ces données ne sont pas pertinentes pour la surveillance de l'utilisation d'Internet et du courrier électronique puisque l'utilisation d'Internet et du courrier électronique au sein de l'administration fédérale génère par principe toujours des données administrées. Il ne pourrait y avoir d'exception que si un organe fédéral prenait des mesures techniques pour l'empêcher. Pour donner un exemple d'une utilisation de l'infrastructure électronique qui ne génère pas de données non administrées, prenons le cas d'une photocopieuse qui n'est pas connectée à un réseau. La photocopieuse dispose d'un disque interne sur lequel différentes données d'utilisation (date, heure, nombre de pages, etc.) sont enregistrées. Quand la capacité d'enregistrement est épuisée, les anciennes données d'utilisation sont écrasées par celles issues de nouvelles photocopies. Après l'écrasement, les anciennes données secondaires ne sont plus disponibles et ne peuvent pour cette raison plus être analysées.

## 11. Conditions de l'analyse

Les exigences applicables aux trois formes d'analyse présentées varient en fonction de l'intensité de l'atteinte aux droits de la personnalité des collaborateurs. Elles figurent dans l'ordonnance sur les données secondaires. Nous nous permettons de préciser ici que l'analyse des données secondaires peut prendre beaucoup de temps et par conséquent aussi coûter cher. Chaque organe fédéral ne devra ainsi pas seulement se demander si les conditions en vue de l'analyse souhaitée sont remplies, mais également si les coûts justifient une telle analyse.

### 11.1 Analyses ne se rapportant pas aux personnes: art. 8 de l'ordonnance sur les données secondaires

L'**exploitant du système** et le **service prévu dans le concept de protection des données de l'organe fédéral** ne peuvent pas effectuer d'analyses de données administrées ne se rapportant pas aux personnes pour tous les buts visés à l'art. 57I, let. b, LOGA. Cette analyse peut être effectuée de manière systématique et sans motif particulier, c'est-à-dire sans limite de temps ni de contenu.



On peut également se demander si la forme de l'analyse peut aussi être ordonnée par l'**organe fédéral**. Une interprétation littérale des dispositions légales aurait pour effet, à la différence de l'analyse non nominale se rapportant aux personnes, que l'analyse pourrait être effectuée uniquement par l'exploitant du système et le service prévu dans le concept de protection des données de l'organe fédéral. Mais cette forme d'analyse doit à juste titre aussi pouvoir être **ordonnée par l'organe fédéral**. La distinction des personnes ou services autorisés à effectuer l'analyse ou à déposer une demande en ce sens ne doit constituer qu'une différenciation par rapport à l'analyse nominale se rapportant aux personnes au sens de l'art. 10 (voir plus bas).

## **11.2 Analyses non nominales se rapportant aux personnes: art. 9 de l'ordonnance sur les données secondaires**

- L'exploitant du système,
- le service prévu dans le concept de protection des données de l'organe fédéral ou
- l'organe fédéral

peuvent, de leur propre chef, procéder à des **analyses par sondage** des données administrées visées à l'art. 57n, let. a et b, LOGA afin de contrôler l'utilisation de l'infrastructure électronique et les heures de travail du personnel. Cette forme d'analyse peut aussi être ordonnée par l'organe fédéral. Il est cependant à souligner que l'analyse non nominale se rapportant aux personnes **ne peut pas être effectuée de manière systématique**.

Dans la pratique, il peut arriver qu'une analyse non nominale se rapportant aux personnes mette en évidence des abus commis par un collaborateur particulier ou par un groupe de collaborateurs. Ce soupçon suffisant peut-il servir de base à une analyse nominale se rapportant aux personnes ? Comme souvent quand il s'agit de protection des données, cette question ne saurait recevoir de réponse générale. Il faut au contraire insister sur le fait que le soupçon doit en tout cas être suffisamment étayé et que l'analyse nominale se rapportant aux personnes doit, sur la base des faits concrets, respecter le principe de la proportionnalité. Il ne faut en outre pas perdre de vue qu'une telle analyse entraîne des coûts élevés.

## **11.3 Analyse nominale se rapportant aux personnes: art. 10, 11, 12 et 13 de l'ordonnance sur les données secondaires**

Comme l'analyse nominale des données secondaires se rapportant aux personnes constitue l'atteinte la plus forte aux droits de la personnalité des employés, les exigences y relatives sont très strictes: les exigences concernant le mandat d'analyse sont expressément réglées dans l'ordonnance sur les données secondaires, une distinction est faite entre trois buts d'analyse différents (sous différentes conditions) et l'analyse peut être effectuée uniquement par des organes fédéraux et après que la personne concernée ait été informée par écrit.

Les buts autorisés de l'analyse nominale se rapportant aux personnes sont mentionnés à l'art. 57o, al. 1, LOGA.

### **11.3.1 Mandats d'analyse nominale se rapportant aux personnes en cas d'utilisation abusive ou de soupçon d'utilisation abusive: art. 10 de l'ordonnance sur les données secondaires**

L'analyse ne peut être effectuée ou ordonnée que par l'organe fédéral pour lequel travaille l'utilisateur de l'infrastructure électronique. Les organes fédéraux qui recourent aux services d'un exploitant de système externe, c'est-à-dire ne faisant pas partie de l'administration fédérale, n'ont ainsi pas le droit de laisser



celui-ci procéder à l'analyse. Les règles contractuelles entre l'organe fédéral et le prestataire de services (personne chargée de traiter les données) ne fait pas de ce dernier un organe fédéral. Le PFPDT refuse toute construction juridique qui ferait d'un prestataire de services externe un auxiliaire de l'organe fédéral. Si un organe fédéral qui se trouve dans cette situation veut analyser de manière nominale les données secondaires se rapportant aux personnes, mais qu'il ne peut ou n'a pas le droit de le faire lui-même, il doit remettre les fichiers journaux à un autre organe fédéral qui est en mesure d'effectuer l'analyse.

Avant cette analyse, la personne concernée doit être informée par écrit (art. 57o, al. 2, let. b, LOGA). Si la personne s'oppose à l'analyse, la direction de l'organe fédéral doit donner son aval. Chaque organe fédéral doit définir qui fait partie de la direction.

Si l'organe fédéral qui a donné le mandat d'analyse dispose d'un conseiller à la protection des données, celui-ci doit **impérativement** recevoir une copie du mandat (art. 10, al. 3, de l'ordonnance sur les données secondaires).

### **11.3.2 Déroulement des analyses nominales se rapportant aux personnes en cas d'utilisation abusive ou de soupçon d'utilisation abusive: art. 11 de l'ordonnance sur les données secondaires**

Avant l'analyse, l'organe fédéral chargé de l'analyse nominale (en général l'OFIT) doit vérifier d'une part que le soupçon concret d'utilisation abusive est motivé par écrit de manière suffisante ou que l'utilisation abusive est prouvée, d'autre part que la personne concernée a été informée par écrit de l'existence d'un soupçon concret ou de la preuve d'une utilisation abusive (art. 11, al. 1, let. a et b, de l'ordonnance sur les données secondaires). En raison de l'énoncé de l'art. 57o, al. 2, let. b, LOGA, il faut aussi vérifier que la personne concernée a été informée par écrit de l'analyse dont ses données vont faire l'objet.

Si l'organe fédéral chargé de l'analyse nominale refuse d'y procéder parce qu'il est d'avis que les conditions (soupçon concret d'utilisation abusive motivé par écrit ou utilisation abusive prouvée, information par écrit de la personne concernée, approbation de la personne concernée ou autorisation de la direction de l'organe fédéral) ne sont pas remplies, l'organe fédéral qui a donné le mandat d'analyse peut demander au PFPDT de prendre position.

Dans ce cas, le PFPDT vérifiera que les conditions relatives à une analyse nominale se rapportant aux personnes sont remplies. Il remettra son avis aux organes fédéraux impliqués et à la personne concernée dans une prise de position écrite. Celle-ci ne constitue cependant pas une décision formelle, puisque le PFPDT n'a aucune compétence en la matière. La prise de position est davantage un avis d'expert auquel les organes fédéraux impliqués et la personne concernée peuvent se référer au cours de la procédure ultérieure.

Pour le cas où l'organe fédéral qui a donné le mandat d'analyse et l'organe fédéral chargé de l'analyse ne font qu'un (comme c'est par ex. le cas au DDPS, à l'OFIT et en principe à chaque endroit où l'organe fédéral est aussi l'exploitant de l'infrastructure électronique), l'art. 11, al. 3, de l'ordonnance sur les données secondaires exige que le **conseiller à la protection des données** de son département soit impérativement informé.



### **11.3.3 Analyses nominales se rapportant aux personnes en vue d'éliminer des perturbations (et de parer à une menace concrète)**

Cette analyse de l'utilisation d'Internet ou du courrier électronique est effectuée pour découvrir quel collaborateur est à l'origine de la perturbation ou de la menace. Il peut s'agir concrètement de constater quel collaborateur a introduit un cheval de Troie dans le système et comment cela a pu se produire, ou quel collaborateur porte atteinte à la bande passante en partageant des fichiers.

L'exploitant et le service prévu dans le concept de protection des données de l'organe fédéral peuvent effectuer cette analyse **de leur propre chef**. Cette réglementation est nécessaire afin que l'exploitant chargé d'assurer le bon fonctionnement de l'infrastructure électronique et d'éliminer les perturbations puisse agir même sans mandat formel de l'organe fédéral. Mais afin que l'exploitant n'effectue pas à sa guise des analyses nominales se rapportant à des personnes, l'art. 12, al. 2, de l'ordonnance sur les données secondaires précise que ces analyses sont uniquement autorisées si:

1. elles sont nécessaires (c'est-à-dire quand le but ne peut pas être atteint par une autre forme d'analyse, moins invasive);
2. l'utilisation de l'infrastructure électronique est impossible ou fortement restreinte en raison d'un défaut ou d'une panne ou parce que les utilisateurs la sollicitent de manière inhabituelle, ou si
3. l'infrastructure électronique ou les données de la Confédération risquent d'être endommagées de manière imminente (diffusion de programmes malveillants).

Nous insistons sur le fait qu'il n'est pas possible d'effectuer sans autres d'analyse nominale se rapportant aux personnes à des fins de surveillance de l'utilisation d'Internet et du courrier électronique dès que les conditions des art. 10, 11 ou 12 de l'ordonnance sur les données secondaires sont remplies. Il faut aussi tenir compte du principe de la proportionnalité et des autres principes inscrits dans la loi sur la protection des données (voir chif. 4.1 à 4.3).

### **11.3.4 Information sur les résultats des analyses**

En vertu de l'art. 15, al. 1, de l'ordonnance sur les données secondaires, l'exploitant du système présente les résultats de l'analyse à l'organe fédéral qui l'a mandaté. En cas d'analyse nominale se rapportant à une personne pour utilisation abusive ou pour soupçon d'utilisation abusive, l'organe fédéral qui a donné le mandat informe la personne concernée des résultats.