Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Préposé fédéral à la protection des données et à la transparence**
**PFPDT**

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

## A l'attention de l'économie privée

État: septembre 2013

Feldeggweg 1, 3003 Berne
Tél. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch

# Table des matières

# Introduction: La surveillance de l’utilisation d’Internet et du courrier électronique au lieu de travail

Le présent guide explique de manière simple et compréhensible aux employeurs et aux employés quelles formes la surveillance de l’utilisation d’Internet et du courrier électronique à des fins d’empêchement d’abus peut prendre et sous quelles conditions elle est licite du point de vue de la protection des données. Les employés étant de plus en plus souvent munis d’appareils de communication mobiles (ordiphones, ordinateurs portables), il convient de souligner que ces appareils sont soumis aux mêmes règles que les postes fixes.

Le présent guide traite concrètement de l’analyse des données secondaires générées lors de l’utilisation d’Internet et du courrier électronique. Les données secondaires sont pour ainsi dire les traces qu’on laisse quand on surfe sur Internet ou écrit des courriers électroniques. Il s’agit ainsi de données journalisées qui indiquent qui a fait quoi et quand, et, dans le cas des courriers électroniques, avec qui.

Il est sûre que les employeurs ont un intérêt important à surveiller l’utilisation que leurs employés font d’Internet et du courrier électronique. Le temps que les employés passent à surfer et à écrire des courriers électroniques à titre privé pendant leurs heures de travail est un facteur de coûts. Il est en outre possible que des employés consultent des sites Internet aux contenus illicites. Il est dans l’intérêt de l’employeur qu’il l’empêche s’il souhaite éviter que sa réputation en pâtisse ou qu’il en soit rendu responsable.

Dans le même temps, il faut rappeler que surveiller l’utilisation que les employés font des moyens de communication est, dans certains secteurs économiques, devenu une obligation pour les employeurs. Mentionnons à titre d’exemple les règles de la Finma sur le comportement des employé(e)s sur le marché financier en relation avec le négoce de valeurs mobilières. La Finma exige clairement que des mesures appropriées soient prises pour empêcher ou détecter l’usage abusif, par des collaborateurs, d’informations confidentielles susceptibles d’influencer les cours. La surveillance des courriers électroniques fait évidemment partie de ces mesures.

En dépit (ou peut-être précisément à cause) de ces évolutions, les employeurs doivent respecter les dispositions réglant la protection des données lorsqu’ils surveillent l’utilisation que les employés font d’Internet et du courrier électronique. Ces dispositions sont exposées et expliquées dans le présent guide.

# 1. 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, 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.

# 2. Données générées lors de l’utilisation d’Internet et du courrier électronique

L’utilisation d’Internet et du courrier électronique laisse des traces à divers endroits. Les outils informatiques utilisés en commun (par ex. les serveurs) établissent en général des fichiers journaux des activités exécutées.

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. Mais les contenus des courriers électroniques sont en partie aussi enregistrés.

La taille des fichiers journaux (voire annexe A) peut rapidement devenir très importante. 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 inter-réseaux (pare-feux ou routeurs) et sur les serveurs de la «zone démilitarisée» (voir plus bas).

Quand un délit a été commis, les données des fichiers journaux des fournisseurs de services Internet (providers) peuvent être examinées moyennant une ordonnance judiciaire.

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 n’est ainsi plus nécessaire d’accéder aux données dans Intranet. 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).

Les données des fichiers journaux sont généralement des données personnelles au sens de la loi sur la protection des données (LPD, RS 235.1). Le traitement de ces données est ainsi soumis aux dispositions de la LPD.

# 3. Principes de la protection des données et bases légales

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. Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées (art. 12, al. 1, LPD). Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. Le traitement des données ne peut se faire sans motifs justificatifs.

Lors du traitement de données personnelles, il faut en outre tenir compte des dispositions générales en matière de protection des données visées aux art. 4 à 11a LPD. Il faut respecter en particulier les principes de la proportionnalité, de la finalité du traitement et de la transparence. L'employeur doit par ailleurs prendre les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données. Il doit aussi pouvoir garantir le droit d'accès. S'il fait réaliser des analyses par des tiers ou des entreprises externes, il doit examiner si cette externalisation est licite et comment il peut y procéder dans le respect des principes de la protection des données. Enfin, il doit tenir compte de l'interdiction de la surveillance du comportement.

Le but de l'employeur doit être d'empêcher ou de mettre au jour des abus.

## 3.1 Licéité

Tout traitement de données doit être licite (art. 4, al. 1, LPD). Le traitement de données personnelles nécessite un motif justificatif, sans quoi il y aurait atteinte illicite à la personnalité (art. 13, al. 1, LPD). D'aucuns sont d'avis que le contrat de travail peut à lui seul constituer un motif justificatif pour l'analyse des données secondaires. C'est vrai dans des domaines particuliers, par exemple dans le secteur bancaire, où il s'impose davantage qu'ailleurs de surveiller les collaborateurs pour lutter contre les délits d'initié, la corruption, etc. Dans les secteurs où la surveillance n'est pas obligatoire, l'employeur peut régulièrement faire valoir un intérêt privé prépondérant. Il n'est ainsi pas obligé de demander son accord à l'employé ☐ accord qui
constituerait un motif justificatif qu'à condition que l'employé l'ait donné volontairement après avoir été informé de manière appropriée. Ce volontariat doit par principe être considéré de manière extrêmement critique dans la mesure où des employés peuvent pour diverses raisons se sentir mis sous pression et limités dans leur liberté.

## 3.2 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 et que l'employeur doit choisir la forme d'analyse qui porte le moins atteinte aux droits de la personnalité des collaborateurs. Cette double obligation se traduit par trois formes fondamentales de l'analyse possibles, qui sont exposées dans le présent guide.

## 3.3 Finalité du traitement

Le principe de la finalité du traitement (art. 4, al. 3, LPD) veut que les données secondaires ne puissent être traitées que dans les buts annoncés aux collaborateurs au moment de la collecte des données. L'employeur satisfait à ce principe en édictant un règlement de surveillance et en traitant les données conformément aux règles fixées. Le règlement définira à quelles analyses il peut être procédé dans quels buts et avec quelles données (fichiers journaux). L'annexe B contient un règlement type de surveillance. Si l'employeur analyse les fichiers journaux dans un but qui n'est pas prévu par le règlement, il enfreint le principe de la finalité du traitement et, par conséquent, les dispositions de la LPD.

## 3.4 Transparence

L'employeur doit satisfaire au principe de la transparence (art. 4, al. 4, LPD) en édictant un règlement de surveillance (sur ce point, voir les explications relatives au règlement d'utilisation). Si l'employeur effectue de telles analyses sans avoir édicté de règlement ni l'avoir fait savoir au personnel, il enfreint la LPD.

Edicter un règlement d'utilisation et le porter à la connaissance des employés participe aussi du principe de transparence.

# 4. Interdiction de la surveillance du comportement

L'art. 26, al. 1, de l'ordonnance 3 relative à la loi sur le travail (OLT 3, RS 822.113) 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 des employés. 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 à des fins de surveillance des comportements d'utilisation. Nous nous empressons d'ajouter qu'il peut cependant y avoir des exceptions à ce principe: dans certains secteurs de l'économie privée (par ex. dans les banques), la surveillance et l'analyse systématiques des courriers électroniques des collaborateurs s'imposent afin que l'entreprise puisse remplir les exigences en matière de conformité et se mettre ainsi à l'abri d'actions en responsabilité.

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 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.

Mais l'interdiction de la surveillance du comportement n'est pas absolue. Il est permis de procéder à des analyses nominales du comportement en cas de soupçon concret ou d'abus avéré.

# 5. Mesures techniques et organisationnelles

## 5.1 Mesures techniques

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

Les employeurs doivent naturellement communiquer à leurs collaborateurs quelles utilisations d'Internet et du courrier électronique sont autorisées et lesquelles ne le sont pas. L'employeur édictera à cet effet un règlement d'utilisation que les collaborateurs devront connaître.

L'authentification et l'autorisation, 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.

**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. 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.

## 5.2 Règlement d'utilisation

L'employeur définit dans le règlement d'utilisation selon quelles modalités les employés peuvent utiliser Internet et le courrier électronique à titre non professionnel. Le droit de donner des instructions selon l'art. 321*d* du code des obligations (CO, RS 220) constitue la base légale à cet effet.

Le règlement d'utilisation (voir annexe B) assure la transparence et la sécurité du droit. Il évite ainsi des discussions superflues entre l'employeur et les employés. Le règlement doit être porté à la connaissance des employés; cela se fera en général par écrit. A des fins de preuve, l'employeur demandera aux employés de confirmer qu'ils ont bien reçu le règlement. Les grandes entreprises publient généralement leurs règlements en ligne; les employés reçoivent un courrier électronique contenant le lien qui mène au règlement d'utilisation, consultable dans le domaine Intranet. Il est permis de procéder aussi de cette manière. L'employeur doit informer les employés de toute modification du règlement.

L'employeur permet normalement aux employés 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'employeur 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 les employés savent ce qui est permis et ce qui est interdit. On évite ainsi les conflits inutiles.

### 5.3 Sécurité des données

Le maître du fichier, dans ce cas l'employeur, doit, en vertu de l'art. 7 LPD, protéger les données personnelles (donc aussi les fichiers journaux) contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées, notamment au moyen d'un système adéquat de rôles et d'autorisations et de la journalisation des accès aux fichiers journaux. Le guide «Mesures techniques et organisationnelles de la protection des données» traite de ce thème de manière approfondie.

### 5.4 Programmes de surveillance

Les programmes de surveillance que l'employeur installe lui-même sur l'ordinateur du collaborateur constitue une atteinte massive aux droits de la personnalité de la personne concernée, car ils 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 pour leur part de consigner tous les textes tapés sur le clavier. En raison de l'atteinte massive aux droits de la personnalité du collaborateur qu'ils constituent, de tels programmes de surveillance ne peuvent être utilisés que moyennant une ordonnance judiciaire.

## 6. Utilisation abusive

Le traitement des données secondaires sert à empêcher ou à mettre au jour des abus. L'employeur définit dans le règlement d'utilisation ce qu'il faut entendre par une utilisation abusive.

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'employeur.
2. Abus en termes qualitatifs: Le collaborateur consulte des sites Internet aux contenus illégaux ou définis comme illicites par l'employeur. Le harcèlement (mobbing) par courrier électronique relève aussi de l'abus en termes qualitatifs.

# 7. Formes d’analyse

L’analyse des données secondaires peut prendre trois formes (voir aussi annexe A). En vertu du principe de la proportionnalité, l’employeur 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 l’employé.

## 7.1 Analyse anonyme (ne se rapportant pas aux personnes)

Les fichiers de données secondaires sont toujours nominaux puisqu’ils fournissent des informations sur les personnes qui les ont générés. Il peut s’agir de l’adresse de courrier électronique du collaborateur, de l’adresse IP ou d’un numéro d’identification. L’analyse anonyme des données secondaires n’implique pas que les données doivent être rendues anonymes avant l’analyse. Elle implique plutôt que 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? Ces analyses peuvent être effectuées de manière systématique même en l’absence d’un soupçon concret d’abus.

## 7.2 Analyse pseudonyme (non nominale se rapportant aux personnes)

Comme nous l’avons dit plus haut, les données brutes (fichiers journaux) sont en rapport direct avec les personnes. 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 semaine? L’employé qui remplit ce critère figurera dans la liste sous un pseudonyme. Ces analyses peuvent être aussi effectuées de manière systématique même en l’absence d’un soupçon concret d’abus.

## 7.3 Analyse nominale se rapportant aux personnes

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’entreprise). Une telle analyse ne peut être effectuée qu’à condition qu’il y ait pour le moins un soupçon concret d’abus ou qu’une analyse non nominale se rapportant aux personnes ait montré qu’un abus a été commis et qu’il faut en identifier l’auteur.

# 8. Autres points importants

## 8.1 Droit d'accès

En vertu de l'art. 8 LPD, toute personne peut demander au maître du fichier, dans ce cas à l'employeur, si des données la concernant sont traitées. L'employeur doit par conséquent communiquer à l'employé qui en fait la demande:

- toutes les données le concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données;
- le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données.

La demande d'accès doit en règle générale être déposée par écrit auprès de l'employeur accompagnée de la copie d'une pièce d'identité. Cela peut sembler superflu en raison de l'existence d'un contrat de travail, mais est cependant recommandé. Si la demande satisfait à ces exigences, l'employeur ne peut pas la rejeter au motif qu'elle présente des erreurs formelles.

L'employeur a 30 jour pour fournir les renseignements ou, au contraire, une décision motivée restreignant le droit d'accès (art. 1, al. 4, OLPD). Les renseignements doivent, en règle générale, être fournis par écrit (art. 8, al. 5, LPD). D'entente avec l'employeur, l'employé peut aussi consulter ses données sur place (art. 1, al. 3, OLPD).

L'employeur peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où:

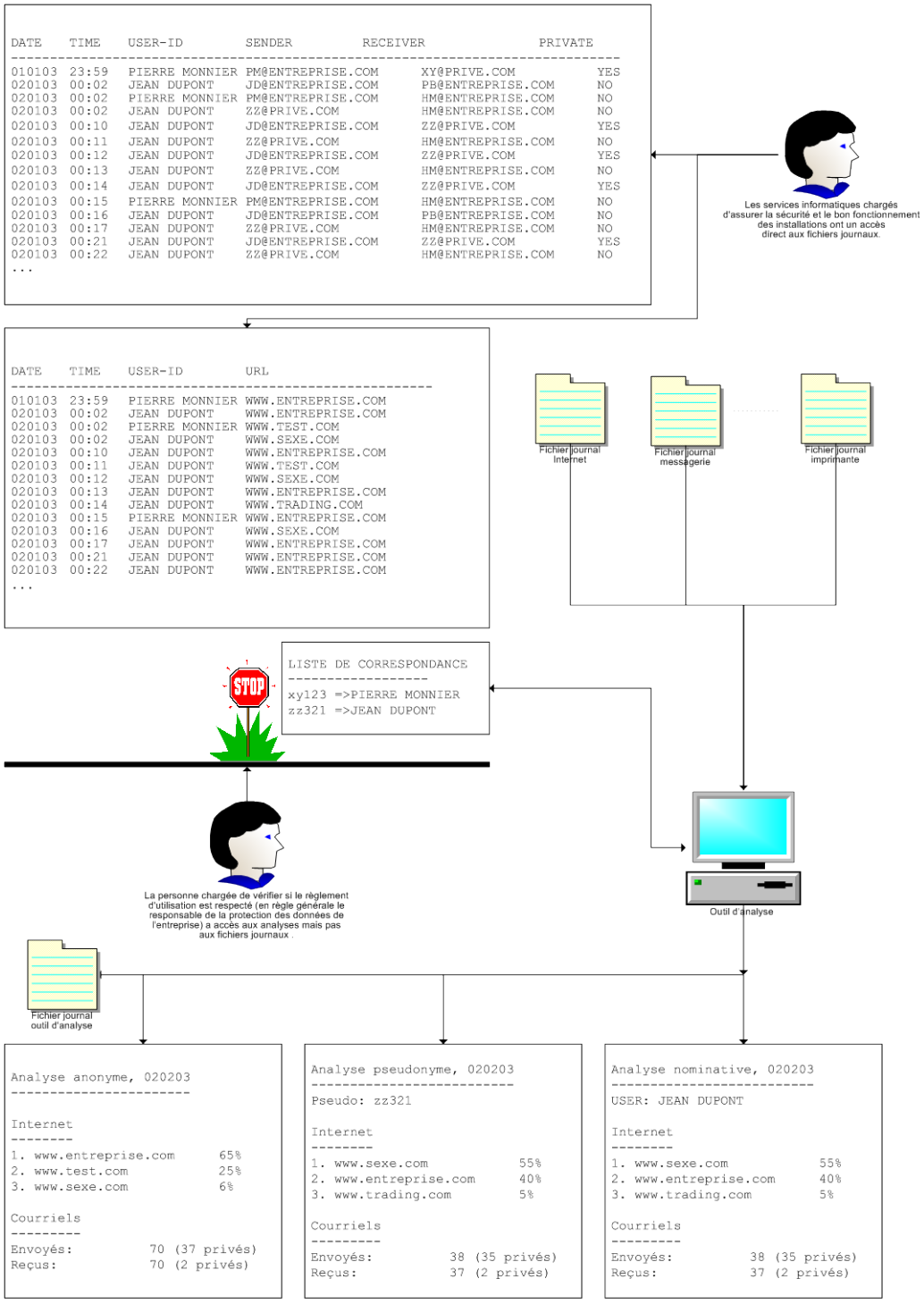
- une loi au sens formel le prévoit;
- les intérêts prépondérants d'un tiers l'exigent, ou dans la mesure où
- ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à un tiers.

L'employeur doit justifier par écrit pourquoi il refuse ou restreint la communication des renseignements demandés, ou en diffère l'octroi (voir plus haut).

## 8.2 Externalisation de l'analyse des données secondaires

De nombreuses entreprises ont externalisé l'intégralité de leurs services informatiques ou ne peuvent (ou ne veulent) pas procéder elles-mêmes à l'analyse des données secondaires pour des raisons de coûts ou parce qu'elles ne disposent pas du savoir-faire requis. L'externalisation de l'analyse des données secondaires ne pose en soi pas de problèmes. Mais l'art. 10a LPD (Traitement de données par un tiers) fixe que le traitement de données personnelles ne peut être confié à des tiers qu'à condition qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise. Il faut examiner dans chaque cas si une obligation légale de garder le secret interdit de transmettre les données au tiers concerné à des fins d'analyse des données secondaires.

# Annexe A: Fichiers journaux et analyse



# Annexe B: Règlement type de surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail

Le texte du règlement est en caractères standard, les notes et les commentaires sont en italique.

## B.1 But et champ d'application

### B.1.1 But

Le présent règlement a pour but de protéger les intérêts de l'employeur et de l'employé dans le contexte de la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail.

### B.1.2 Champ d'application

Le présent règlement s'applique à tout employé, interne ou externe, de l'entreprise.

## B.2 Intérêts et risques de l'employeur et de l'employé

### B.2.1 Intérêts et risques de l'employeur

L'utilisation, au lieu de travail, d'un ordinateur en réseau peut porter atteinte à certains intérêts et équipements techniques de notre entreprise. Peuvent être affectés:

- la capacité de stockage et la bande passante du réseau, suite à une utilisation excessive d'Internet et du courrier électronique;
- 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 à l'entreprise;
- le temps de travail et d'autres intérêts financiers (pertes de productivité, augmentation des coûts pour des moyens et/ou prestations supplémentaires, frais de réseau, etc.);
- d'autres intérêts de l'entreprise protégés par la loi, tels que sa réputation, ses secrets de fabrication ou d'affaires, ou encore la protection des données.

### B.2.2 Intérêts et risques de l'employé

L'employé encourt certains risques en cas d'utilisation abusive, par exemple sur le plan du droit du travail (les sanctions peuvent aller jusqu'au licenciement) et, partant, sur le plan économique. Mais il prend aussi des risques du point de vue du droit de la protection des données même quand il ne fait rien d'illicite: des informations personnelles contenues dans des courriers électroniques peuvent par exemple être utilisées à des fins abusives.

## B.3 Mesures de protection techniques et journalisations

### B.3.1 Mesures de protection techniques

L'entreprise met en œuvre les mesures de protection techniques suivantes:

- ...

- ...

- ...

### B.3.2 Journalisations

La plupart des activités effectuées à l'aide de moyens informatiques sont consignées dans des fichiers journaux. La journalisation est l'enregistrement continu des données d'utilisation de type «qui, quoi, quand». Dans notre entreprise, elle est effectuée aux endroits suivants:

- ...

- ...

- ...

*On indiquera ici les types de journalisation effectués, le but visé, le contenu et la durée de conservation des données. L'entreprise remplira ainsi le devoir d'information qui lui incombe en vertu de l'art. 4, al. 2, LPD en matière de traitement de données et de constitution de fichiers.*

Les fichiers journaux relatifs aux messages privés ne comprennent que l'adresse de l'employé, la mention «Privé», la date et l'heure d'envoi ou de réception du message.

## B.4 Règlement d'utilisation

*C'est à l'employeur de décider si les employés peuvent utiliser Internet et le courrier électronique à des fins privées au lieu de travail. Comme dans les autres domaines du rapport de travail, il dispose en effet du droit d'établir des directives. La portée des droits d'utilisation pourra varier selon les catégories d'employés et selon les besoins de chacun sur le plan professionnel.*

*Des règles concrètes et dénuées de toute ambiguïté doivent être fixées dans ce chapitre. Le règlement d'utilisation doit être mis à jour si nécessaire.*

## B.5 Règlement de surveillance

### B.5.1 Priorité aux mesures de protection techniques

Notre entreprise s'engage à privilégier les mesures de protection techniques pour prévenir les abus et les dommages de nature technique.

Elle actualise régulièrement les mesures de protection techniques en fonction des évolutions de la technologie. Elle adapte également ces mesures après un dérangement technique.

Elle n'a le droit de procéder à une analyse nominale des fichiers journaux de l'utilisation d'Internet et du courrier électronique que dans les cas où les mesures de protection techniques ne suffisent pas à empêcher un abus.

Elle n'utilise pas d'espiogiciels.

### B.5.2 Analyse des fichiers journaux

L'entreprise effectue des analyses anonymes et pseudonymes des fichiers journaux dans le but de vérifier si le règlement d'utilisation est respecté.

L'analyse anonyme est une analyse statistique des fichiers journaux qui s'effectue sur la base des critères suivants: *(L'entreprise indiquera ici les critères qu'elle a retenus)*.

L'analyse pseudonyme se fait par sondages uniquement. *L'entreprise indiquera ici le calendrier et la période pendant laquelle le sondage aura lieu*.

Les analyses pseudonymes (ou anonymes) portent sur des échantillons suffisamment grands de personnes pour garantir le caractère pseudonyme (ou anonyme). Les fichiers journaux et les listes de correspondance sont conservés séparément, par des personnes ayant des fonctions différentes.

Si notre entreprise constate un abus lors d'une analyse anonyme ou pseudonyme (ou qu'une analyse fait naître un soupçon d'abus), elle procède à une analyse nominale des fichiers journaux en utilisant la liste de correspondance. Est considérée comme abus toute violation du règlement d'utilisation.

S'il s'avère qu'un soupçon est infondé, l'entreprise interrompt immédiatement l'analyse nominale.

*On indiquera ici la personne responsable de l'analyse nominale. En règle générale, cette tâche sera assumée par le conseiller à la protection des données de l'entreprise.*

Si l'analyse des fichiers journaux ou d'autres éléments révèlent l'existence d'un délit ou font naître des soupçons d'abus, l'entreprise sauvegarde les fichiers journaux concernés. Elle se réserve le droit de déposer plainte contre la personne concernée. La suite de la procédure relève des autorités pénales. L'entreprise s'engage à traiter les résultats de l'enquête de manière confidentielle, notamment à l'égard des tiers non autorisés (tels que les autres collaborateurs de l'entreprise).

*C'est le supérieur hiérarchique – et non le service informatique – qui décidera si une plainte est déposée ou non. Bien qu'il n'existe aucune obligation en la matière, il est recommandé de le faire, du moins pour les délits poursuivis d'office, afin d'écarter le risque que l'entreprise ne soit déclarée complice.*

### B.5.3 Surveillance exercée dans le but de garantir la sécurité et le bon fonctionnement du système informatique ou sur la base d'autres indices

Si l'entreprise constate un dysfonctionnement du système informatique en dépit des mesures de protection techniques prises, elle peut analyser les fichiers journaux pour en déterminer la cause.

Si le dysfonctionnement est dû à un abus, le collaborateur fautif peut faire l'objet d'une des sanctions visées au point B 5.8.

Si l'employeur constate un abus ou s'il pense qu'il y a eu abus parce que d'autres indications le lui font supposer, il peut consulter les fichiers journaux concernés et leurs analyses. En cas d'abus, il peut prononcer l'une des sanctions visées au point B 5.8.

### B.5.4 Distinction entre courriers électroniques privés et courriers électroniques professionnels

Les courriers électroniques privés doivent être signalés en tant que tels (option «Privé») par l'expéditeur, que ce dernier fasse partie de l'entreprise ou non.

L'entreprise n'a le droit ni de consulter ni de traiter d'une quelconque manière les courriers privés signalés comme tels.

Lorsque rien n'indique la nature (professionnelle ou privée) du courrier et que les éléments d'adressage ne permettent pas non plus de déterminer qu'il s'agit d'un courrier privé, l'entreprise part de l'idée qu'il s'agit d'un courrier de nature professionnelle. En cas de doute, l'employeur clarifie la question avec l'employé. Les expéditeurs, internes ou externes, doivent être expressément informés sur ce point.

L'entreprise vous recommande d'utiliser un service web de courrier électronique si possible chiffré, afin de mieux protéger vos courriers privés.

*Le droit d'utiliser un service web de courrier électronique chiffré dépend de ce que prévoit le règlement d'utilisation. S'il est interdit d'utiliser Internet à titre privé, cette possibilité n'existe pas.*

*En vue de mieux distinguer le courrier professionnel du courrier privé, l'entreprise pourra aussi décider que le courrier électronique de nature professionnelle soit envoyé avec des adresses fonctionnelles plutôt que nominatives.*

### B.5.5 Surveillance du courrier électronique de nature professionnelle

L'entreprise a le droit d'établir des fichiers journaux pour les courriers d'ordre professionnel et, si nécessaire, de sauvegarder ces messages.

Ces fichiers journaux englobent notamment le champ «Objet», la date et l'heure d'envoi ou de réception du courrier, l'adresse de l'expéditeur et celle du destinataire.

### B.5.6 Gestion du courrier électronique d'un collaborateur absent

Pour les absences prévisibles (telles que vacances, congés ou service militaire) comme d'ailleurs imprévisibles (maladie ou accident), l'employé désigne un suppléant qui aura le droit de lire et, si nécessaire, de traiter les courriers professionnels entrants.

Le suppléant n'aura pas accès aux courriers signalés comme privés.

Les expéditeurs externes de courriers privés doivent être informés du fait que les courriers privés non signalés comme tels sont susceptibles d'être lus par le suppléant.

### B.5.7 Gestion du courrier électronique d'un collaborateur ayant quitté l'entreprise

L'employé qui va quitter l'entreprise doit, avant son départ, transférer à qui de droit les affaires et les courriers électroniques en suspens.

Il certifie par une déclaration qu'il a remis à l'entreprise tous les documents de nature professionnelle.

On doit lui offrir la possibilité de copier ses messages électroniques et autres documents privés sur un support privé, puis de les effacer des serveurs de l'entreprise.

A la fin du dernier jour de travail au plus tard, son compte de courrier électronique (comme du reste ses autres comptes informatiques) sera bloqué et sa boîte de messagerie (comme tous les autres supports de données personnels), effacée. En cas de décès, le compte de courrier électronique du défunt sera immédiatement bloqué et les données seront sauvegardées.

Les personnes qui enverront un message à l'adresse bloquée seront automatiquement informées du fait que cette adresse n'existe plus. La réponse automatique pourra en outre leur indiquer une adresse de remplacement.

### B.5.8 Sanctions en cas d'abus

Si les conditions requises pour la surveillance et les règles qui la régissent ont été respectées, l'entreprise est en droit, lorsqu'elle constate un abus, de prendre des sanctions disciplinaires contre l'employé fautif.

*On énumèrera ici les sanctions possibles: avertissement, blocage de l'accès à Internet, demande de dommages-intérêts, suppression de primes, etc. Dans les cas extrêmes, par exemple si l'abus se reproduit malgré un avertissement et provoque une panne technique ou si un délit est prouvé, l'employeur peut congédier l'employé. Le contrat de travail peut cependant être résilié avec effet immédiat uniquement lorsqu'en toute bonne foi on ne peut plus exiger de l'employeur qu'il maintienne les rapports de travail. Les sanctions doivent être adaptées à la gravité de l'abus et avoir été définies préalablement.*

### B.5.9 Prétentions de l'employé en cas de surveillance illicite

Si les conditions requises pour la surveillance et les règles qui la régissent ne sont pas respectées, l'employé peut faire valoir les prétentions prévues par le code civil en cas d'atteinte à la personnalité (cf. art. 28 ss CC).

En cas de surveillance abusive par l'entreprise, l'employé peut aussi engager une poursuite pénale contre elle, par exemple pour violation du domaine secret ou du domaine privé au moyen d'un appareil de prises de vues (art. 179$^{quater}$ CP) ou pour soustraction de données personnelles (art. 179$^{novies}$ CP).

### B.5.10 Autres dispositions

Les employés de notre entreprise sont régulièrement sensibilisés, par divers cours, aux risques en rapport avec l'utilisation d'Internet et du courrier électronique.

Les services informatiques et les responsables hiérarchiques de l'entreprise prennent toutes les mesures techniques nécessaires pour empêcher que les données personnelles qu'ils traitent dans le cadre d'une surveillance tombent entre les mains de personnes non autorisées.

Ils veillent en particulier à assurer la confidentialité, la disponibilité et l'intégrité de ces données.

L'employé peut en tout temps demander à l'entreprise si des données le concernant sont traitées et, le cas échéant, lesquelles.

Des données personnelles ne peuvent être communiquées à des tiers non autorisés sans motif valable ou sans l'accord de la personne concernée. Les collègues de travail de la personne concernée sont considérés comme des tiers.

L'entreprise n'a aucune obligation légale de conserver les fichiers journaux. Elle peut toutefois le faire pendant une durée limitée (ne dépassant en général pas quatre semaines) s'ils sont susceptibles de servir de moyens de preuve.

La durée de conservation dépendra du but de la journalisation. Dans le cadre d'une procédure de sanction ou d'une procédure pénale, les fichiers journaux pourront être conservés jusqu'à l'expiration du délai de recours correspondant.