

**Yves Lasfargue**

**Internet et libertés dans l'entreprise**

# **INTERNET, DROITS DES SALARIES ET INTRANETS SYNDICAUX**

***6 fiches pédagogiques***

**O**bergo

OBservatoire des conditions de travail et de l'ERGOstressie



Mise à jour permanente de cette  
brochure sur le site :  
[www.ergostressie.com](http://www.ergostressie.com)

Yves LASFARGUE

# *Internet, droits des salariés et intranets syndicaux*

*Version du 1er février 2008*

***Droits d'utilisation des informations et des documents publiés sur le site [www.ergostressie.com](http://www.ergostressie.com)***

Toutes les informations et les documents du site [www.ergostressie.com](http://www.ergostressie.com) peuvent être utilisés gratuitement sans aucun droit à payer à deux conditions : l'indication de la source (Nom de l'auteur : Yves Lasfargue et adresse du site [www.ergostressie.com](http://www.ergostressie.com)) est obligatoire et l'utilisation doit être non commerciale (interdiction de revendre ou de diffuser les documents à titre commercial).



L'ensemble de cette création logicielle est mis à disposition sous un [contrat Creative Commons](http://creativecommons.org)  
(voir tous les détails sur le site : <http://creativecommons.org>)

© 2008 - Yves Lasfargue

"Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droit, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal. La loi du 11 mars 1957 n'autorise, aux termes des alinéas 2 et 3 de l'article 41, que les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective d'une part, et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration".

© Yves Lasfargue – 2008

# Sommaire

## **PARTIE 1 :**

### **6 fiches sur les droits des salariés, internet, et intranets : les différents points à négocier** **7**

Fiche 1 - Consultation obligatoire du CE avant la mise en place du projet " Intranet DRH"	8
Fiche 2 - Consultation obligatoire du CE avant la diffusion de la charte "Intranet"	10
Fiche 3 - Négociations de l'utilisation par le Comité d'Entreprise de l'intranet DRH	12
Fiche 4 - Négociations de l'utilisation par les organisations syndicales de l'intranet	13
Fiche 5 - Modalités de respect des libertés individuelles et collectives	18
Fiche 6 - Négociations des conditions de travail sur internet / intranet	23

## **PARTIE 2 :**

### **Conception et utilisation des sites intranet et internet syndicaux : vers un syndicat à accès multiple (SYAM)** **27**

1 - Les 2 canaux internet : informations "poussées" et informations "tirées"	28
2 - Nécessité de multiplier les canaux : vers le SYAM?	29
3 - Quelques idées pour l'utilisation de la messagerie	29
4 - Quelques idées pour la conception et l'utilisation des sites syndicaux	30
5 - Quelques idées pour l'utilisation du téléchargement	32
6 - Quelques idées pour l'utilisation des forums	32
7 - Les moyens nécessaires	32

## **ANNEXES** **33**

### **Annexe 1 : Bibliographie et liens** **33**

### **Annexe 2 : textes commentés (Chartes, accords et arrêts concernant internet et intranet)** **35**

Annexe 2 – 1 : Exemple de charte d'utilisation des TIC	35
Annexe 2 – 2 : Recommandations interministérielles du 19 juin 2001	43
Annexe 2 – 3 : Exemple d'accord sur l'intranet syndical : accord France Télécom	49
Annexe 2 – 4 : Présentation rapide de quelques accords	53
Annexe 2 – 5 : Quelques arrêts de la Cour de cassation	54
Annexe 2 – 6 : Décret du 20 octobre 2005 sur les correspondants à la protection des données	58

### **Annexe 3 : textes internationaux commentés** **65**

Annexe 3 – 1 : Convention du Conseil de l'Europe sur la cybercriminalité (8 novembre 2001)	65
--	----

### **Annexe 4 : propositions syndicales** **74**

Annexe 4 – 1 : 12 propositions de la CFDT Cadres (12 février 2002)	74
--	----



**Yves Lasfargue**

- Chercheur et consultant, directeur de l'OBERGO (**OB**servatoire des conditions de travail et de l'**ERGO**stressie)
- Membre du groupe de réflexions sur les enjeux du « E-Travail » (créé par le Ministère du Travail et de l'Emploi)

1996-2005 : - Membre du Conseil scientifique de l'ANACT (Association Nationale pour l'Amélioration des Conditions de Travail)

1993/2000 : directeur du Créfac (**CentRe d'Étude et de Formation pour l'Accompagnement des Changements**)

1999/2000 : Président du groupe de travail "Nouvelles technologies, qualifications et formations dans le Secteur Public" du Commissariat Général du Plan et expert auprès du Comité Economique et Social européen.

1998/1999 : Animateur du groupe "Commerce électronique et emplois" de la mission Lorentz (Ministère de l'Économie)

1996/1998 : Membre du groupe d'experts de haut niveau de la Communauté européenne, à Bruxelles, chargés d'étudier les effets sociaux et sociétaux de la Société de l'Information.

*Ouvrages déjà publiés par Yves Lasfargue :*

- **Ordinateurs, gestion et entreprises** (Hachette Formation Conseil -1972)
- **Ordinateurs pour la gestion** (De Vecchi -1978) - Prix AFIN 1978 (Association française des informaticiens)
- **Une informatique par et pour les gestionnaires** (Les Editions d'Organisation - 1980)
- **L'avenir de la robotique** - rapport du Conseil Economique et Social, dont Y.Lasfargue était le rapporteur (Les Editions d'Organisation-1982)
- **Travailler dans l'informatique : rêves et possibilités** (Documents APEC - Association pour l'emploi des cadres - Les Editions d'Organisation - 1987)
- **Vivre l'informatique** (Les Editions d'Organisation -1984 - 5ème édition en 1991)
- **Techno jolies, techno folies ? Comment réussir les changements technologiques** (Les Editions d'Organisation - 3ème tirage en 1991)
- **Robotisés ? Rebelles ? Rejetés ? Maîtriser les changements technologiques** (Les Editions de l'Atelier -1993)
- **Techno mordus, Techno exclus? Vivre et travailler à l'ère du numérique** - (Les Editions d'Organisation/ Les Echos - Paris - 2000).
- **Halte aux absurdités technologiques** - (Les Editions d'Organisation - Paris - 2003).
- **Kit 2008 de mesure de la qualité de vie au travail dans la société de l'information** - (téléchargeable gratuitement sur le site [www.ergostressie.com](http://www.ergostressie.com)).

*Ouvrages et rapports officiels auxquels Yves Lasfargue a participé :*

- **L'état des sciences et des techniques** (La Découverte -1983 et 1991)
- **Prospectives 2005** - Commissariat Général du Plan et CNRS (Économica 1987)
- **Le travail en puces** - ouvrage collectif sous la direction de Danièle Linhart et Jacques Perriault - PUF 1992 (Nouvelle Encyclopédie Diderot)
- **Construire la société européenne de l'Information pour tous** - rapport établi par 14 experts pour la Commission Européenne en avril 1997 (DG V). Rapport disponible en français, anglais et allemand sur internet ([www.europa.eu.int](http://www.europa.eu.int))
- **La nouvelle donne du Commerce électronique** - rapport de la mission Lorentz du Ministère de l'Économie, des Finances et de l'Industrie (mars 1999). Les Editions de Bercy - Rapport disponible en français sur internet ([www.internet.gouv.fr](http://www.internet.gouv.fr)).
- **L'État et technologies de l'information et de la communication : vers un service public "à accès multiple"** - rapport de la mission Lasserre du Commissariat Général du Plan - Documentation Française - mars 2000 ([www.internet.gouv.fr](http://www.internet.gouv.fr))

	<b>«Un grand coup d'air frais sur la pensée unique qui entoure parfois les nouvelles technologies. »</b>	
	Le Nouvel Observateur du 5 juin 2003 <b>"Un livre brûlot contre " le technologiquement correct"</b>	
	01 Informatique du 2 mai 2003 <b>« C'est un nouveau pavé dans la mare. Qui possède un triple mérite. Primo, l'ouvrage est agréable à lire. Secundo, il évite les pièges de la technophobie. Tertio, il est concret, tout est argumenté et documenté, avec notamment des témoignages de professionnels et d'experts. Une lecture profitable pour les managers et les directeurs de ressources humaines »</b>	
	L'Usine Nouvelle du 29 mai 2003 <b>« Yves Lasfargue dénonce aujourd'hui le discours de ceux qui voudraient imposer à tous l'utilisation d'Internet »</b>	
	L'Express du 29 mai 2000 <b>« Quant aux autres, ils ne devraient pas manquer de regarder désormais d'un tout autre oeil l'écran gris de leur micro-ordinateur " - Le Monde du 13 mai 2003</b>	
	Le Monde du 13 mai 2003 <b>«Et on ne peut que vous conseiller de lire l'ouvrage d'Yves Lasfargue, ... »</b> Le Monde Informatique du 20 juin 2003	
		<p><b>"Halte aux absurdités technologiques"</b> Yves Lasfargue Editions d'Organisation – 2003 238 pages - 22 € ISBN : 2-7081-2915-5</p>

# **PARTIE 1**

## **6 Fiches**

### **« Droits des salariés, internet, et intranets » : les différents points à négocier**

On peut repérer 6 thèmes de discussions et/ou négociations induits par la mise en place des réseaux intranet dans l'entreprise :

**Fiche 1 - Mise en place du projet " Intranet DRH"**

Consultation préalable obligatoire du Comité d'Entreprise

**Fiche 2 - Diffusion de la charte "Intranet"**

Consultation préalable obligatoire du Comité d'Entreprise

**Fiche 3 - Utilisation par le Comité d'Entreprise de l'intranet DRH**

Négociation des modalités

**Fiche 4 - Utilisation par les organisations syndicales de l'intranet**

Négociation des modalités

**Fiche 5 - Respect des libertés individuelles et collectives:**

Négociation des modalités

**Fiche 6 - Conditions de travail sur internet / intranet :**

Analyse des temps et de la charge de travail et négociations

## **Fiche 1 - Mise en place du projet " Intranet DRH"**

Consultation préalable obligatoire du Comité d'Entreprise

Il est évident que la mise en place d'un projet d'intranet, quel que soit le thème de l'intranet (commercial, technique, DRH, ...) est un changement important : le CE doit être consulté (article L 432-2 du Code du Travail), et il peut faire jouer son droit d'expertise (article L-434-6 du Code du Travail).

### **Textes de base dans le code du travail :**

Article L432-2 du Code du Travail (concerne "tout projet important")

*Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences quant aux points mentionnés ci-dessus. Lorsque l'employeur envisage de mettre en œuvre des mutations technologiques importantes et rapides, il doit établir un plan d'adaptation. Ce plan est transmis, pour information et consultation, au comité d'entreprise en même temps que les autres éléments d'information relatifs à l'introduction de nouvelles technologies. En outre, le comité d'entreprise est régulièrement informé et périodiquement consulté sur la mise en œuvre de ce plan.*

Article L432-2-1 du Code du Travail (concerne "les traitements automatisés de gestion du personnel")

*Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de ceux-ci. Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.*

Article L434-6 du Code du Travail (concerne le recours à une expertise technologique)

...

*Le comité d'entreprise, dans les entreprises d'au moins trois cents salariés, peut, en outre, avoir recours à un expert à l'occasion de tout projet important dans les cas énumérés à l'article L. 432-2. Cet expert dispose des éléments d'information prévus à ce même article.*

On voit que la nécessité de consultation du Comité d'Entreprise et le droit d'expertise supposent que le projet:

- \* introduise de nouvelles technologies dans l'entreprises (c'est vrai pour tout projet intranet)
- \* soit important
- \* ait des incidences sociales (c'est vrai pour tout projet intranet, particulièrement un intranet DRH)

La difficulté est d'identifier le "projet intranet" car il commence souvent par une suite d'expérimentations de faible importance dont les impacts deviennent peu à peu significatifs: le CE doit demander à être consulté le plus tôt possible, et en tout cas dès que cette importance est visible (nombre de personnes utilisant la messagerie, nombre de pages du site intranet, importance des informations publiées sur le site,...). Les CE doivent être très attentifs à ce type de projets, même si au début ne semblent se poser ni problèmes d'emploi, ni problèmes de conditions de travail: l'enquête " Liaisons sociales - France Télécom " (voir en bibliographie) a montré qu'une forte proportion d'entreprises n'a pas procédé à cette consultation alors que 60% estiment que l'intranet DRH induit un changement important dans l'organisation du travail.

### ***Que trouve - t - on dans un " Intranet DRH"?***

Aujourd'hui existent deux grands types d'intranets dans les entreprises

a) Les sites intranets " professionnels " spécialisés par fonction et à accès limités, qui sont ou devraient être des outils de " partage de connaissances ":

- Intranet commercial
- Intranet technique
- Intranet DRH : accessible aux services DRH seulement

- b) Le site intranet DRH " grand public " pour l'ensemble des salarié(e)s

A l'utilisation de ce site intranet DRH, viennent s'ajouter :

- L'utilisation de la messagerie pour l'envoi d'informations individuelles ou collectives
- L'utilisation du site internet de l'entreprise par la GRH pour le public extérieur, en particulier pour présenter les offres d'emplois.

Les principaux services que l'on peut trouver sur un site intranet DRH sont les suivants :

### **1 Intranet DRH = outil de publication (journal ou panneau d'affichage)**

- Des informations générales sur l'actualité de l'entreprises
- Des informations sur les services pratiques
- Des informations sur le droit du travail: convention collective, règlement intérieur, notes de services ,...
- Des informations pour la formation : catalogue, calendrier,...
- Des outils informations pour la mobilité interne : bourse de l'emplois,...
- Des informations pour la mobilité externe
- Des informations sur les recrutements et offres d'emplois
- Des informations ciblées par catégories de salarié(e)s : expatriés,... - ...

### **2 Intranet DRH = outil d'échanges des salarié(e)s avec RH et avec les autres salariés**

- Annuaire de l'entreprise donnant l'adresse électronique des autres salariés
- Messagerie avec réponse personnalisée et rapide - ....

### **3 Intranet DRH = outil permettant au salarié de gérer son dossier personnel**

- Des outils interactifs (personnalisés et sécurisés) pour la gestion des frais
- Des outils interactifs (personnalisés et sécurisés) pour la gestion du temps de travail
- Des outils interactifs (personnalisés et sécurisés) pour la gestion de la paie, de l'épargne salariale, de la prévoyance,...

### **4 Intranet DRH = outil de formation**

- Des outils de gestion des compétences (test,...)
- Des outils de formation à distance (e-learning) - ...

### **5 Intranet DRH = outil de publication pour le Comité d'Entreprise**

- Informations sur les œuvres sociales
- Gestion plus ou moins interactives des activités (réservations, billets,...)
- ...

**ATTENTION !!! Ce type d'utilisation par le CE doit toujours être explicitement négocié sous peine de nombreux conflits.**

## Fiche 2 - Diffusion de la « charte Intranet »

Liaisons avec le règlement intérieur et le contrat de travail

La « charte Intranet », appelée aussi "Charte d'utilisation des moyens informatiques ou "Charte des moyens de communication ", souvent rédigée en grande partie par le service informatique, définit les modalités d'utilisation des moyens informatiques en général, et des réseaux internet / intranet en particulier, pour tous les salariés.

Elle est parfois considérée comme un document technique permettant la sauvegarde technique du système (logiciels utilisés, taille des messages,...) : en réalité, c'est souvent une modification du règlement intérieur qui doit être traitée comme telle (consultation des différentes instances représentatives).

Article L122-36 du Code du Travail

*Le règlement intérieur ne peut être introduit qu'après avoir été soumis à l'avis du comité d'entreprise ou, à défaut, à l'avis des délégués du personnel ainsi que, pour les matières relevant de sa compétence, à l'avis du comité d'hygiène et de sécurité. Le règlement intérieur doit indiquer la date à partir de laquelle il entre en vigueur . Cette date doit être postérieure d'un mois à l'accomplissement des formalités de dépôt et de publicité. En même temps qu'il fait l'objet des mesures de publicité, le règlement intérieur, accompagné de l'avis du comité d'entreprise ou, à défaut, des délégués du personnel et, le cas échéant, du comité d'hygiène et de sécurité, est communiqué à l'inspecteur du travail. Les dispositions prévues aux alinéas précédents sont applicables en cas de modification ou de retrait des clauses du règlement intérieur.*

### **Articulation "charte/règlement intérieur / contrat de travail / accord"**

Dans les faits, on trouve 4 niveaux de documents sur lesquels peuvent figurer les droits et les devoirs des salariés dans l'utilisation d'internet et d'intranet :

- \* **Le contrat de travail** : pour les nouveaux embauchés il comporte, en plus du traditionnel rappel au respect du règlement intérieur, une obligation de respect de la "Charte intranet" et parfois des modalités particulières à certains emplois ou à certaines fonctions (utilisation de micro-ordinateurs portables en dehors de l'entreprise,...).
- \* **Le règlement intérieur** : il définit les droits et devoirs de chaque salarié(e), et est souvent complété par des articles spécifiques à l'utilisation des systèmes de traitement de l'information et de communication.
- \* **La charte intranet**: elle définit les modalités d'utilisation des moyens informatiques en général, et des réseaux internet / intranet en particulier, pour tous les salariés.
- \* **L'accord d'utilisation d'intranet par les organisations syndicales** : elle définit les modalités d'utilisation des moyens informatiques en général, et des réseaux internet / intranet en particulier, pour les organisations syndicales.

### **Que peut - on trouver dans une charte intranet?**

Les chartes sont très variées selon qu'elles ont été écrites plutôt par des informaticiens, plutôt par le service juridique ou plutôt par la DRH.

Son objectif est d'assurer la sécurité et le bon fonctionnement du système d'informations de l'entreprise, et le respect des libertés individuelles de chaque salarié.

On trouve souvent les points suivants (voir un exemple de charte, très complète, commentée en annexe 2 – 2.) :

- les règles générales d'utilisation des systèmes de traitement de l'information et de communication
- les mesures de sécurité et les conseils de vigilance
- Les normes : matériels et logiciels à utiliser
- Le traitement des virus : que faire en cas de virus?
- Les règles d'utilisation spécifiques aux différentes fonctions : messagerie, téléchargement,...
- Parfois : les sanctions encourues en cas de non respect (mais la charte devient alors un sous-ensemble du règlement intérieur)

**Attention ! Certains articles des chartes déjà en vigueur sont devenus illégaux depuis l'arrêt de la Cour de cassation du 2 octobre 2001 concernant l'impossibilité pour l'entreprise de consulter les fichiers identifiés comme étant « personnels » des salarié(e)s. Voir l'annexe 2 - 4.**

### *Chaque salarié doit-il signer individuellement la charte?*

Certaines entreprises, en particulier les filiales des groupes anglo-saxons, demandent aux salariés de signer individuellement la charte. Souvent, seule une petite partie des salariés signent...

Pourquoi les entreprises veulent-elles des signatures individuelles? En général, c'est pour avoir la preuve que les méthodes de contrôle n'ont pas été mises en place à l'insu des salarié(e)s : chaque salarié, par sa signature, reconnaît avoir été informé (respect des articles L121-7 et L121-8 du Code du Travail)

## Fiche 3 - Utilisation par le Comité d'Entreprise de l'intranet DRH

### Négociation des modalités

Pas de texte législatif spécifique, pour le moment, concernant l'utilisation de l'intranet par le Comité d'Entreprise.

Mais cette utilisation existe déjà dans certaines entreprises à la suite d'accords implicites ou explicites : l'entreprise met à la disposition du Comité d'Entreprise pour afficher les principales "activités sociales " (voyages, vacances, arbre de Noël, bibliothèque, randonnées,...) proposées par le Comité d'Entreprise.

Cet affichage d'activités "non conflictuelles" est intéressant, car il peut permettre une certaine appropriation des outils par les membres du CE. Mais il faut être conscient que rapidement de nombreuses questions se posent :

- \* Quels nouveaux moyens sont mis à la disposition du CE (matériels, logiciels, formation, personnel supplémentaire,...)?
- \* Modalités des mises à jour? "Censure préalable" avant la diffusion des informations?
- \* Liens avec les sites Web internes (intranet) ou externes (internet) des organisations syndicales?
- \* Possibilité de diffusion des comptes rendus du CE sur le site intranet (site sécurisé accessible aux seul(e)s salarié(e)s)?
- \* Possibilité de diffusion des comptes rendus des commissions ?
- \* Possibilité de diffusion des réponses aux questions posées par les Délégués du Personnel?
- \* Utilisation du site en période d'élections pour présenter le bilan et les candidatures?
- \* Utilisation du site en période de conflits ?

**C'est pourquoi, ce type d'utilisation par le Comité d'Entreprise doit toujours être explicitement négocié sous peine de voir se développer de nombreux conflits qui vont paralyser la diffusion des informations du CE.**

Cette négociation est différente de celle concernant l'utilisation de l'intranet par les organisations syndicales, mais lui est liée de très près.

Cette négociation doit être aussi liée à la mise en place de la "charte intranet"

### ***Quels sont les points à négocier pour l'utilisation de l'intranet par le Comité d'Entreprise?***

Ce sont les mêmes que ceux concernant l'utilisation par les organisations syndicales, mais en général les entreprises sont beaucoup plus "permissives" pour la diffusion des informations « sociales et tourisme » du comité d'entreprise qu'elles ne le sont dans les négociations pour la diffusion d'informations syndicales:

- 1) Utilisation de la messagerie électronique
- 2) Utilisation d'un site Web intranet
- 3) Utilisation du téléchargement
- 4) Utilisation de forum de discussions
- 5) Utilisation du " chat " ou messagerie instantanée
- 6) Utilisation de l'internet
- 7) Moyens mises à la disposition du Comité d'entreprise

On trouvera le détail des points à négocier dans la fiche n°4 sur l'utilisation par les organisations syndicales.

## Fiche 4 - Utilisation par les organisations syndicales de l'intranet

Négociation des modalités des intranets syndicaux

Le seul texte législatif spécifique, pour le moment, concernant l'utilisation de l'intranet par les organisations syndicales est l'article 52 de la loi n° 2004-391 du 4 mai 2004 qui a complété l'article L 428 du Code du travail.

D'autre part, l'accord français sur le télétravail du 25 septembre 2005 fait allusion aussi aux intranets syndicaux.

L'article L. 412-8 du code du travail est maintenant ainsi rédigé depuis le 4 mai 2004 :

*L'affichage des communications syndicales s'effectue librement sur des panneaux réservés à cet usage et distincts de ceux qui sont affectés aux communications des délégués du personnel et du comité d'entreprise.*

*Un exemplaire de ces communications syndicales est transmis au chef d'entreprise, simultanément à l'affichage. Les panneaux sont mis à la disposition de chaque section syndicale suivant des modalités fixées par accord avec le chef d'entreprise.*

*Les publications et tracts de nature syndicale peuvent être librement diffusés aux travailleurs de l'entreprise dans l'enceinte de celle-ci aux heures d'entrée et de sortie du travail.*

*Le contenu de ces affiches, publications et tracts est librement déterminé par l'organisation syndicale, sous réserve de l'application des dispositions relatives à la presse.*

*Dans les entreprises de travail temporaire, les communications syndicales portées sur le panneau d'affichage doivent être remises aux salariés temporaires en mission ou adressées par voie postale, aux frais de l'entrepreneur de travail temporaire, au moins une fois par mois.*

*Un accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique de l'entreprise.*

*Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne pas entraver l'accomplissement du travail.*

*L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message.*

Ce texte complète la réponse du gouvernement à une question écrite au Parlement :

*« Il appartient aux organisations syndicales de rechercher, par voie d'accord avec l'employeur, les modalités d'accès à la messagerie générale et de diffusion des messages à caractère syndical sur celle-ci... même si, l'intranet ayant vocation à être un instrument strictement professionnel, aucune disposition ne contraint l'employeur à accorder aux organisations syndicales l'accès à ce réseau. » (JO du 1<sup>er</sup> Février 1999).*

### Article 11 - Droits collectifs

Les télétravailleurs ont les mêmes droits collectifs que les salariés qui travaillent dans les locaux de l'entreprise, notamment en ce qui concerne leurs relations avec les représentants du personnel et l'accès aux informations syndicales, y compris par les intranet syndicaux dans les mêmes conditions que les autres salariés

*(Extrait de l'accord national sur le télétravail du 25 septembre 2005).<sup>1</sup>*

<sup>1</sup> Voir la brochure « Négocier le télétravail » publiée par l'OBERGO (téléchargeable gratuitement sur le site [www.ergostressie.com](http://www.ergostressie.com))

Il existe déjà des accords dans certaines entreprises<sup>2</sup> (exemples : France Télécom, Technip, Groupama, Renault,...). Voir l'annexe 2 et en particulier l'accord France Télécom (annexe 2 - 3)

Pour la fonction publique, ont été publiées les recommandations interministérielles du 19 juin 2001 sur l'utilisation des TIC par les organisations syndicales. Ces recommandations, qui serviront à l'élaboration de chartes ministérielles, visent à permettre aux organisations syndicales de bénéficier des nouvelles technologies pour simplifier leur tâche quotidienne et enrichir le dialogue social. Voir le texte intégral en annexe 2 - 2 .

### ***Principes des accords sur l'utilisation de l'intranet par les organisations syndicales***

Il s'agit de respecter et de trouver un équilibre entre:

- les règles de sécurité de fonctionnement du système de communication et de traitement des informations de l'entreprise
- les droits et possibilités d'expression des organisations syndicales
- les règles de confidentialité permettant des respecter les libertés individuelles et collectives

En général, le principe d'un accord est le suivant :

- \* l'entreprise négocie un certain nombre d'utilisations possibles de l'intranet par les organisations syndicales
- \* en contrepartie, l'organisation syndicale s'engage à respecter les règles fixées par la charte de fonctionnement, en particulier les règles de sécurité.

C'est pourquoi, la plupart de ces accords sont des accords bilatéraux entre l'entreprise et chaque organisation syndicale. Contrairement aux accords traditionnels (toutes les organisations syndicales et l'entreprise signent ensemble le même document), chaque organisation syndicale s'engage sur un document séparé (identique pour toutes les organisations syndicales) avec l'entreprise.

### ***Principaux points à aborder dans les accords***

Il faut remarquer que la discussion sera d'autant plus fructueuse que les négociateurs, représentant l'entreprise ou les syndicats, auront un bon niveau d'appropriation des outils intranet. Les 7 points suivants doivent être abordés dans les accords :

- 1) Utilisation de la messagerie électronique
- 2) Utilisation d'un site Web intranet
- 3) Utilisation du téléchargement
- 4) Utilisation de forum de discussions
- 5) Utilisation du " chat " ou messagerie instantanée
- 6) Utilisation de l'internet par l'organisation syndicale
- 7) Moyens mises à la disposition des organisations syndicales

#### **1) Utilisation de la messagerie électronique**

1 - 1 Types d'envois de messages possibles : à qui ? combien ? Quand ?

- \* Possibilités d'envois de tracts?
- \* Possibilités de "SPAM" (Technique d'envoi en masse de publicités par courrier électronique utilisée par la publicité classique) sans que cet envoi ait été sollicité par les destinataires.

En général, ce type d'envois n'est pas autorisé par les accords (voir par exemple l'accord France Télécom): seul est autorisé le courrier "normal" ou parfois le "courrier aux adhérents".

Il faut remarquer que le "courrier aux adhérents" est dangereux : la liste d'envois est une liste des adhérents connue de l'entreprise.

<sup>2</sup> Deux documents CFDT très intéressants sur l'ensemble de ces sujets :

\*" *Internet/Intranet et droit syndical - Guide d'action syndicale BETOR PUB CFDT* ".

Document édité par le BETOR PUB (Fédérations des Services CFDT) : (juin 2000)

Yvan Béraud - 01 42 03 89 55 Courriel : info@betor-pub.org

\* « *Intranet : accès et usages arbitraires* » - Magazine Célidé pour les Comités d'Entreprise - n°21 d'août / septembre 2001 (www.celide.asso.fr)

1 - 2 Respect des règles de fonctionnement prévues pour les autres utilisateurs (en général marquées dans la "Charte Intranet" et/ou le règlement intérieur)

- \* Taille des messages
- \* Taille et format des pièces jointes
- \* Respect des règles de sécurité (mots de passe,...)

1 - 3 Gestion de la transparence (tout ce qui est transmis par internet ou intranet peut être transparent pour les techniciens du système).

Cette transparence concerne deux points principaux:

- \* Confidentialité du contenu des messages (voir la fiche 5 sur les libertés)
- \* Confidentialité du flux des messages: qui écrit à qui? Quand? Combien de fois?

Attention ! Jugement important ! La Cour d'appel de Paris a jugé<sup>3</sup> que l'envoi d'un message syndical par la messagerie intranet, qui n'est utilisable que pendant les heures de travail, constituait, en l'absence d'un accord d'entreprises ou d'usage dérogatoire, une transgression évidente des conditions posées par l'article L.412 - 8 du Code du travail relatif à la diffusion d'informations syndicales dans l'entreprise.

## 2) Utilisation d'un site Web intranet

2 - 1 Contenus du site Web

En général, le contenu est laissé sous la responsabilité de chaque organisation syndicale selon les règles et coutumes des panneaux d'affichage. Mais sont peu prises en compte les spécificités d'un "tableau d'affichage" sur intranet. Par exemple sont souvent interdites:

- \* Utilisation de l'interactivité (forum de discussion, téléchargement, ou possibilité par l'internaute d'utiliser des programmes interactifs du genre "calcul des impôts" en partant de données fournies par l'utilisateur)
- \* Utilisation de fichiers multimédia (sons, musiques, vidéo,...)
- \* Utilisation de cookies (petits fichiers stockés sur le micro-ordinateur de l'internaute facilitant l'utilisation du site)
- \* Utilisation de liens possibles avec d'autres sites internes ou externes?

2 - 2 Contraintes techniques

- \* Taille maximale du site Web (volumes d'informations stockées sur le site) : souvent ce volume est limité à des volumes ridiculement faibles de 5, 10 ou 20 méga octets, alors que n'importe quel internaute peut profiter de 100 méga octets chez n'importe quel hébergeur de site!
- \* Type de serveur d'hébergement : le site peut être hébergé sur le site de l'intranet DRH ou sur un serveur spécifique aux organisations syndicales.
- \* Modalités de mise à jour : l'organisation syndicale peut mettre à jour directement son site (bonne solution pour des raisons de délais et d'autonomie) ou doit passer par les services de l'entreprise

2 - 3 Gestion de la transparence des appels

Tout ce qui est transmis par internet ou intranet peut être transparent pour les techniciens du système.

- \* Confidentialité de l'audience : combien d'appels par jour? Par mois?  
Évidemment cette information est fondamentale et intéresse chaque organisation syndicale : les modalités de diffusion doivent être négociées. Par exemple, le taux d'audience du site intranet syndical (regroupant les sites des 6 organisations syndicales) est diffusé comme l'est le taux d'audience des autres sites intranet.
- \* Confidentialité de l'origine des appels: qui a appelé le site? Quand? Combien de fois?

<sup>3</sup> Cour d'appel de Paris – 14<sup>ème</sup> chambre B, 31 mai 2002

Ce type d'informations ne doit pas être calculée afin de sauvegarder les libertés individuelles de salarié(e)s.

### **3) Utilisation du téléchargement**

Le téléchargement de fichiers en partant d'un site Web est une fonction très utile: l'utilisateur ne télécharge que les fichiers qui l'intéresse. Contrairement au fichier envoyé en pièce jointe par messagerie (l'utilisateur reçoit le fichier sans l'avoir demandé), le fichier téléchargé est le résultat d'un choix de l'utilisateur.

L'utilisation du téléchargement est, pour le moment, interdite dans la plupart des accords, comme l'est l'utilisation de toutes les possibilités d'interactivités.

### **4) Utilisation de forum de discussions**

Le forum est une utilisation interactive du site. Un forum de discussion est une messagerie publique où apparaissent les messages de tous les participants : questions posées par l'animateur du forum ou par les participants; réponses apportées par l'animateur du forum ou par les participants. En général on crée un forum sur un thème de discussion précis. Sur internet, il existe des milliers de forums différents. Sur les intranets, il existe souvent des forums sur des thèmes professionnels : forum commercial; forum sur un projet particulier, forum technique sur une famille de produits...

Le forum est un outil d'échanges intéressant surtout quand il est animé par un modérateur qui recadre les débats et ne publie que les échanges ayant un certain intérêt.

L'utilisation des forums est, pour le moment, interdite dans la plupart des accords, comme l'est l'utilisation de toutes les possibilités d'interactivités.

### **5) Utilisation du " chat " ou messagerie instantanée**

Cette messagerie instantanée: chaque participant (en général 2, mais il est possible d'utiliser de telles messageries à plusieurs) voit sur l'écran l'affichage instantané du message de son interlocuteur et peut y répondre instantanément.

L'utilisation de la messagerie instantanée est, pour le moment, interdite dans la plupart des accords, comme l'est l'utilisation de toutes les possibilités d'interactivités.

### **6) Utilisation de l'internet par l'organisation syndicale**

L'utilisation de l'internet est évidemment totalement libre et peut être réalisée sans négociation avec l'entreprise. Chaque organisation peut créer un site librement.

Mais il est parfois intéressant de négocier des modalités permettant une utilisation meilleure du site internet:

- Possibilités de faire figurer des informations syndicales sur le site internet de l'entreprise
- Prise en charge par l'entreprise des moyens de connexion à internet (matériels, abonnements, coûts des connexions téléphoniques)
- Prise en charge par l'entreprise des coûts de fabrication et maintenance du site internet

### **7) Moyens mis à la disposition des organisations syndicales**

Faire fonctionner un intranet syndical (messagerie + site Web) coûte cher.

C'est pourquoi, la plupart des accords prévoient des moyens supplémentaires pour permettre aux organisations syndicales de faire fonctionner l'intranet syndical.

7 - 1 Moyens matériels :

- \* Au moins deux micro - ordinateurs par lieu syndical (usine, siège,...) : un micro-ordinateur connecté au réseau intranet et un micro-ordinateur connecté à internet (ce ne peut être le même pour des raisons de sécurité pour l'entreprise, et de confidentialité pour le syndicat).

- \* Des périphériques nécessaires : imprimante; scanner (pour les illustrations et photos,...)
- \* Logiciels : un éditeur de pages HTML (exemple : Dreamwaever), des logiciels de présentation graphiques de sites traitements des photos, des graphiques,...)
- \* Prise en charge des connexions intranet et internet

#### 7 - 2 Moyens financiers :

- \* Pour disposer de personnels supplémentaires de réalisation de sites
- \* Pour l'aides d'experts extérieurs éventuels
- \* Pour faire réaliser la première version du site (qui sera ensuite mis à jour par des moyens internes)

#### 7 - 3 Moyens de formation :

### **Ce sont LES PLUS IMPORTANTS : SANS MOYEN PAS DE SITE INTRANET ATTRACTIF !**

- \* Formation à l'utilisation de la messagerie et à la navigation dur internet / intranet pour tous les responsables syndicaux (si cette formation n'est pas généralisée à l'ensemble du personnel)
- \* Formation à la réalisation de sites pour ceux et celles qui seront responsables de la fabrication et de la mise à jour du site

### **8) Signature par les organisations syndicales**

Dans certaines entreprises, l'employeur signe un accord spécifique avec chaque organisation syndicale, et non pas un accord commun signé par les différentes organisations syndicales. Le Tribunal de grande instance de Nanterre<sup>4</sup> a estimé que la CGT pouvait utiliser l'intranet Renault bien qu'elle n'ait pas signé l'accord ; mais qu'elle devait respecter la charte d'utilisation.

---

<sup>4</sup> Tribunal de grande instance de Nanterre – 31 mai 2002

## Fiche 5 - Respect des libertés individuelles et collectives:

Négociation des modalités

### *Contraintes techniques et lutte contre la cyber criminalité*

Pour la gestion de la sécurité du réseau (surveillance des virus, mesure des flux et des temps de réponse, suivi des pannes...) l'administrateur de réseau doit connaître et enregistrer tous les flux : cela est indispensable pour la gestion du réseau.

L'administrateur de réseau peut aussi connaître le CONTENU des messages : cela n'est pas indispensable pour la gestion du réseau, mais est techniquement possible, sauf si les messages sont cryptés avec un logiciel de cryptage inconnu de l'administrateur de réseau. Cela veut dire que sur internet et intranet tout peut être techniquement transparent.

## Sur internet et intranet, toute utilisation laisse des « traces » et tout peut être TECHNIQUEMENT TRANSPARENT

### **L'administrateur de réseau peut-il prendre connaissance du contenu des messages ?**

**Oui**, précise l'arrêt de la Cour d'appel de Paris du 17 décembre 2001 (11<sup>ème</sup> chambre, section A) :

*"Il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité, ce qui entraîne, entre autres, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter les démarches inutiles. Ils ont donc un accès courant au réseau sans avoir besoin d'une quelconque manœuvre."*

Par contre, cet arrêt confirme la condamnation de l'administrateur de réseau pour avoir divulgué à ses supérieurs ce qu'il avait lu.

Cet arrêt semble donc donner un statut particulier à l'administrateur de réseau : il serait "habilité" à lire les contenus à condition de ne pas les divulguer...

Cette habilitation, si elle était confirmée, poserait de nombreux problèmes de conscience aux administrateurs de réseaux et devrait être négociée avec soin dans les entreprises.

On trouvera le texte intégral de cet arrêt sur le site du " Forum des droits sur l'internet" :

<http://www.foruminternet.org/> et en particulier à l'adresse :

<http://www.foruminternet.org/texte/documents/jurisprudence/lire.phtml?id=240&>

### *Trouver un juste équilibre entre respect des libertés et lutte contre la cyber criminalité*

Le problème est de maîtriser les utilisations possibles de ces informations, qui de toute manière seront enregistrées.

Les textes légaux concernant cette gestion de la transparence, qui doivent permettre un équilibre entre les besoins de sécurité de l'entreprise et le respect des libertés individuelles et collectives ne tiennent pas toujours compte des spécificités nouvelles d'internet, mais constituent une base solide pour traiter ces problèmes.

On trouvera en bibliographie un certain nombre de rapports et textes officiels qui abordent ces problèmes sur le plan mondial, européen, ou français.

### *Une entreprise peut - elle contrôler l'activité d'un(e) salarié(e) en contrôlant son utilisation d'internet / intranet ?<sup>5</sup>*

<sup>5</sup> Un livre indispensable : "Le droit du travail à l'épreuve des TIC" - Jean- Emmanuel Ray - Editions Liaisons - Paris - Depuis 2001 : mise à jour chaque année

Par exemple : en mesurant les flux de messages envoyés, en contrôlant les sites appelés, en mesurant le temps passé à utiliser les différentes possibilités d'intranet et internet, en lisant le contenu des messages électroniques. Les principaux textes légaux applicables sont inscrits dans le Code civil, le Code du travail et le Code Pénal et font apparaître que :

- tout contrôle effectué à l'insu du salarié est illégal. L'entreprise doit respecter la transparence des méthodes de contrôle : ce contrôle est interdit s'il est fait à l'insu du salarié, c'est à dire sans que celui-ci ait été préalablement informé (articles L121-7 et L121-8 du Code du Travail)

- tous les types de contrôle ne sont pas légaux, même après information des salarié(e)s, car l'entreprise ne doit pas apporter de restrictions "non justifiées" aux libertés individuelles et collectives (articles L120-2 du Code du Travail). Le chef d'entreprise peut être condamné pénalement s'il porte atteinte au respect de la vie privée (article 226 - 1 du Code Pénal) ou au secret des correspondances ( article 266 - 15 du Code Pénal).

- les contrôles doivent être cohérents avec les finalités des déclarations de traitements et fichiers effectuées auprès de la CNIL (Commission nationale de l'informatique et des libertés).L'entreprise doit avoir déclaré tous les fichiers et les applications réelles doivent correspondre aux finalités déclarées. Le chef d'entreprise peut être condamné pénalement s'il ne respecte pas la loi "Informatique et libertés"(article 226 - 16 à 226 -21 du Code Pénal)

Attention !!! Il ne faut pas confondre la loi française (qui pour le moment ne comporte aucun article concernant spécifiquement la surveillance des courriers électroniques) et la loi anglaise (en application depuis le 24 octobre 2000) qui permet aux employeurs de lire le courrier électronique et les communications des salariés, même à leur insu.

## **Très important !!!**

### ***Problèmes posés par la pénétration de la vie privée dans la vie professionnelle et de la vie professionnelle dans la vie privée***

\* Arrêt de la cour de Cassation du 2 octobre 2001 sur la confidentialité des messages électroniques (extraits de cet arrêt dit arrêt « Nikon » + commentaires en annexe 2 - 4)

*"... le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, que celle-ci implique en particulier le secret des correspondances, que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur, "*

\* Arrêt de la cour de Cassation du 2 octobre 2001 sur le télétravail subi

\* Arrêt de la cour de Cassation du 17 juillet 2001 sur l'extension du lieu de travail (accident dans une chambre d'hôtel)

\* Arrêt de la cour de Cassation du 17 mai 2005 qui précise que l'employeur ne peut lire un « dossier personnel » mémorisé dans un ordinateur de l'entreprise qu'en présence du salarié :

*« Sauf risque ou évènement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. »*

## **1 - Principe de transparence des méthodes de contrôle**

Tout contrôle effectué à l'insu du salarié est illégal.

Article L121- 7 du Code du Travail

*Le candidat à un emploi est expressément informé, préalablement à leur mise en oeuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard. Le salarié est informé de la même manière des méthodes et techniques d'évaluation professionnelles mises en oeuvre à son égard. Les résultats obtenus doivent rester confidentiels. Les méthodes et techniques d'aide au recrutement ou d'évaluation des salariés et des candidats à un emploi doivent être pertinentes au regard de la finalité poursuivie.*

Article L121- 8 du Code du travail

*Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.*

## **2 - Limites aux restrictions apportées aux libertés individuelles et collectives**

Mais tous les types de contrôle ne sont pas légaux, même après information des salarié(e)s..

Article L120-2 du Code du Travail

*Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.*

## **3 - Atteinte à l'intimité de la vie privée**

Article 8 – de la Convention européenne des droits de l'homme

Droit au respect de la vie privée et familiale

*1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

*2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. <http://www.justice.gouv.fr/textfond/europ1.htm>*

Article 9 du Code civil

*Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.*

Article 226-1 du Code pénal

*Est puni d'un an d'emprisonnement et de 300 000 F d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui : 1 En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; 2 En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.*

## **4 - Secret des correspondances véhiculées par des réseaux de télécommunications**

Article 226-15 du Code pénal

*Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 300 000 F d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.*

## 5 - Applications de la loi " Informatique et libertés " sur les fichiers (Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004)

Les contrôles doivent être cohérents avec les finalités des déclarations de traitements et fichiers effectuées auprès de la CNIL (Commission nationale de l'informatique et des libertés).

### **MISES A JOUR IMPORTANTE EN 2004 ET 2005 DE LA LOI « INFORMATIQUE ET LIBERTES » !!!**

#### **Possibilité de création d'un correspondant à la protection des données dans chaque entreprise**

La loi n° 2004-801 du 6 août 2004, loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, a modifié la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

En particulier, elle a allégé les modalités de déclaration des fichiers à la CNIL en dispensant les entreprises de déclarer leurs fichiers si elles ont désigné un correspondant chargé d'assurer la protection des données :

Nouvelle rédaction de l'article 22 - III de la loi n° 78-17 du 6 janvier 1978 :

*« Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.*

*La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.*

*Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. »*

*(Voir en annexe 2-6 l'analyse du décret du 20 octobre 2005 concernant les correspondants à la protection des données)*

Rappel des articles Code pénal

### **Section 5 Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques**

#### **Art. 226-16**

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

#### **Art. 226-16-1 A**

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

#### **Art. 226-16-1**

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

#### **Art. 226-17**

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

**Art. 226-18**

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

**Art. 226-18-1**

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

**Art. 226-19**

Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

**Art. 226-19-1**

En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende le fait de procéder à un traitement :

1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

**Art. 226-20**

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

**Art. 226-21**

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

## **Fiche 6 - Conditions de travail sur internet / intranet : comment mesurer la pénibilité ?**

Analyse des temps et de la charge de travail

On constate que dans chaque entreprise, le travail est changé par une centaine d'innovations: innovations venant de l'extérieur ou innovations décidées par l'entreprise (commerciales, organisationnelles, technologiques ou sociales).

L'intranet fait partie de l'ensemble des facteurs<sup>6</sup>.

### ***1 - Les 12 évolutions du travail***

Cet ensemble d'innovations induit 12 tendances dans l'évolution du travail et des métiers qu'il nous faut apprendre à gérer... et à négocier.<sup>7</sup>

- 1) Vers un travail de plus en plus ABSTRAIT: le travail s'effectue sur la représentation de la réalité apparaissant sur l'écran informatique (en général, textes écrits) et non plus sur la réalité.

*Nombreux travaux assis devant l'écran et nouvelles répartitions entre ORAL et ECRIT :*

- accélération du passage de l'oral à l'écrit (mouvement qui dure depuis longtemps)
- développement d'un langage entre l'écrit et l'oral (messageries, SMS,...)
- développement d'un nouvel "oral à distance" avec les plates-formes téléphoniques pour certaines applications (ventes, conseils, dépannages,...)

- 2) Vers un travail de plus en plus INTERACTIF: le travail consiste en un "dialogue" homme /machine pendant une grande partie de la journée (40% des utilisateurs de micro-ordinateurs restent plus de 4 heures par jour devant un écran).

- 3) Vers un travail exigeant une gestion de l'ABONDANCE de plus en plus complexe. Nous savons tout numériser vite et pas cher, et le nombre de données numérisées mises à notre disposition augmente chaque jour: des milliards de pages sont déjà accessibles sur Internet, et ce nombre croît régulièrement.

*Sur le plan organisationnel, il faut donc gérer cette abondance de données, pouvant aller jusqu'à la saturation en distinguant soigneusement les concepts suivants (que les membres de la cyber secte ont tendance à confondre) :*

- DONNÉES
- INFORMATIONS (ce qui réduit l'incertitude)
- CONNAISSANCES
- DÉCISIONS
- ACTIONS

*Les TIC donnent à chacun la possibilité d'être à la fois utilisateur et producteur d'informations numérisées. Contrairement à la robotique ou à l'informatique traditionnelle, outils d'automatisation, Internet et les TIC sont rarement des outils de productivité par substitution d'activités automatiques à des activités humaines, mais sont plutôt des outils d'amélioration de la qualité du système d'information.*

- 4) Vers un travail exigeant une GESTION DU TEMPS de plus en plus délicate, car les innovations technologiques donnent la possibilité de travailler plus rapidement. Ceci rejoint la demande des clients et des citoyens qui est de diminuer en permanence les délais de traitement et de réponses.

*Sur le plan organisationnel, il est important de connaître les limites de ces évolutions dans la conception des métiers et la division du travail. En effet, souvent on constate que plus les technologies sont rapides, plus leur utilisation est CHRONOPHAGE :*

- temps d'exploitation de plus en plus long car abondance des données
- temps de bricolage / dépannage de plus en plus long car complexité
- temps d'apprentissage de plus en plus long car diversité des fonctions

<sup>6</sup> Ces évolutions sont détaillées dans le livre "Halte aux absurdités technologiques" - Yves Lasfargue - Editions d'Organisation Paris - 2003 et dans la brochure «Evolutions du travail : présentation du concept d'ergostressie, syndrome de la société de l'information» téléchargeable gratuitement sur le site [www.ergostressie.com](http://www.ergostressie.com)

<sup>7</sup> "Le travail en questions. Enquêtes sur les mutations du travail" - CFDT - Syros - 2001

- différences de temps entre temps du citoyen ou du consommateur (demande de disponibilité totale à toute heure...) et temps du producteur
- différences entre temps Internet et temps biologique

- 5) Vers un travail sur des systèmes de plus en plus VULNÉRABLES. , d'où la nécessité de savoir gérer les nombreux aléas (pannes, intrusions, virus, attaques frauduleuses,...) et de savoir lutter contre les fraudes

*Sur le plan organisationnel, la gestion de la panne sera l'une des activités les plus importantes de la société de l'information. En effet, la généralisation de systèmes complexes est une source de pannes, **car la panne est consubstantielle à la complexité** (pannes techniques et pannes liées à la cyber criminalité : intrusions, virus, attaques frauduleuses,...).*

*En mettant en place de la complexité, des réseaux, des systèmes intégrés, on ne va pas vers le "zéro panne" mais vers le milliard de pannes. Ce qui était vrai pour les ateliers de production dès 1985 (robotique) est aujourd'hui de plus en plus vrai dans le tertiaire et dans les bureaux : **on est passé de la civilisation de la peine à la civilisation de la panne**. Cette nouvelle situation doit être gérée d'autant plus qu'il est très difficile, pour un salarié, de supporter la panne de son matériel en présence de public. Ceci doit avoir des conséquences sur l'organisation (prévoir des systèmes en "mode dégradé") et sur la formation.*

- 6) Vers un travail en LOGIQUE CONTRACTUELLE, car tous les logiciels informatiques sont des outils de « logique contractuelle ».

*Les entreprises de certains pays fonctionnent depuis longtemps selon la "logique contractuelle" (USA, pays anglo-saxons, pays d'Europe du Nord,...): bien travailler, c'est respecter, à la lettre, le contrat passé par exemple entre le chef et le collaborateur Dans les pays "à logique de l'honneur" (pays latins, dont la France), bien travailler c'est essayer de comprendre l'esprit du contrat et "faire différemment, mais mieux"*

*Logique contractuelle = Respect de la LETTRE du contrat toujours explicite.*

*Logique de l'honneur = Respect de l'ESPRIT du contrat explicite ou implicite*

- 7) Vers un travail en QUALITÉ "TENDUE": il faut gérer l'ensemble "flux tendu + qualité totale + flexibilité".

- 8) Vers un travail en RESEAUX et en équipes VIRTUELLES à distance

*Les réseaux donnent la possibilité de réaliser de nombreuses activités à distance : télétravail, travail nomade, télé formation ou e-learning, e-commerce, télé médecine, ...*

*L'analyse des expériences actuelles montre que les activités "à distance" doivent toujours s'accompagner d'activités de proximité en groupes réels avec des participants physiquement présents. Ces regroupements, jadis spontanés, doivent être organisés car ils ont tendance à disparaître avec les outils de communication mobiles. D'autre part, il va falloir apprendre à gérer les communications transversales qui viennent compléter ou perturber les traditionnelles communications verticales*

- 9) Vers un travail exigeant une GESTION DE L'ESPACE de plus en plus délicate:

*Il va aussi falloir apprendre à gérer l'interpénétration **vie professionnelle / vie privée**.*

*D'où l'importance de l'évaluation de la répartition des temps que nous avons vue précédemment et de la définition de règles claires par les partenaires sociaux, la loi et la jurisprudence*

- 10) Vers un travail exigeant la gestion de la TRANSPARENCE et de l'INSTANTANÉITÉ car toute activité effectuée sur un réseau électronique peut être enregistrée à distance.

*Sur le plan social, la gestion de la transparence et de l'instantanéité induites par l'ensemble « système numérisé + réseau » doit être négociée afin qu'elles ne deviennent pas des outils de contrôle social insupportable (traçabilité des produits, mais aussi de l'activité des salariés)*

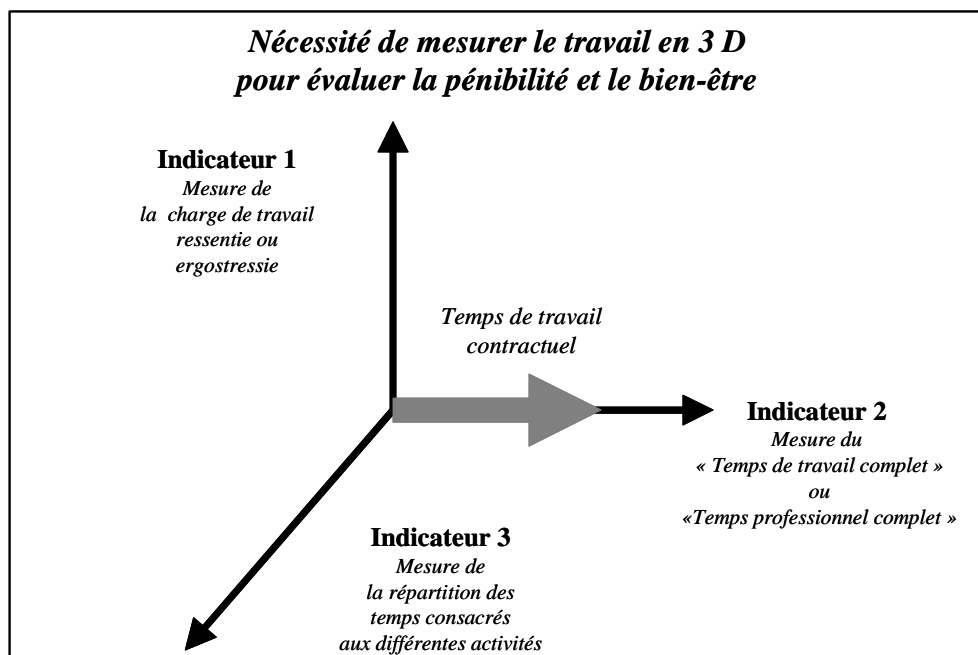
- 11) Vers un travail reposant sur une AUTONOMIE croissante (gestion par objectifs), mais accompagnée de CONTROLES de plus en plus nombreux et de plus en plus permanents.

- 12) Vers une CYBER HIÉRARCHIE, car le rôle des cadres est remis en question.

Au total, le travail que l'on vit dans la société de l'information est très différent de celui que l'on vit dans la société industrielle :

- a) il induit souvent plus de fatigue mentale et de stress que de fatigue physique (mais celle-ci ne disparaît pas!).
- b) Les frontières travail / non-travail ont tendance à s'estomper avec la multiplication des outils portables et la diversité des lieux de travail.

C'est pourquoi, nous proposons de compléter l'indicateur « Temps de travail contractuel » par 3 nouveaux indicateurs permettant d'analyser le travail en 3 D.



La pénibilité et le bien-être au travail résultent de la combinaison de ces 3 indicateurs<sup>8</sup>.

<sup>8</sup> On trouvera sur le site [www.ergostressie.com](http://www.ergostressie.com) le système expert LUCIDITY 1, 2, 3 © donnant un exemple de méthode de mesure de ces 3 indicateurs en partant des tests d'autoévaluation. L'usage du système expert sur Internet et le téléchargement des différents questionnaires d'autoévaluation rassemblés dans le « Kit de mesure de la pénibilité et du bien être dans la société de l'information » sont totalement gratuits.

**-Indicateur n°1 : "charge de travail ressentie"**. Il faut essayer de mesurer les effets sur la santé et le bien être des nouveaux types de travail induits par les activités de la société de l'information en évaluant la charge de travail ressentie. Cette mesure peut se faire en évaluant le niveau d'ERGOSTRESSIE<sup>9</sup>, c'est-à-dire la combinaison de la fatigue physique, de la fatigue mentale, du stress<sup>10</sup> et du plaisir.

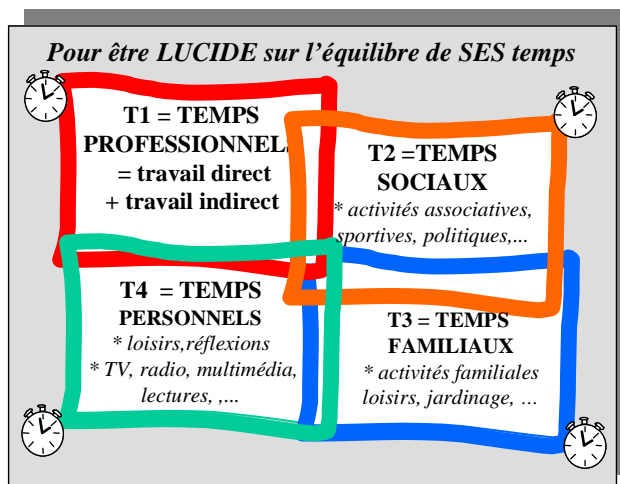


**L'ergostressie est le syndrome de la société de l'information**

*En partant de 100 facteurs, l'autoévaluation de l'ergostressie permet de prendre conscience des principaux facteurs qui agissent sur les conditions de travail et sur le "bien être".*

**- Indicateur n 2 : évaluation de son "temps complet de travail"**. Ce temps est de plus en plus différent du temps de présence dans l'entreprise avec l'interpénétration vie professionnelle/vie privée.

**- Indicateur "Répartition des temps consacrés aux différentes activités"**. Cet indicateur permet analyser la répartition de ses activités entre les différents lieux et temps de vie. A chacun de vérifier en fonction de ses propres objectifs que certaines activités, en particulier les activités familiales et locales, ne sont pas submergées par les activités professionnelles.



### Répartition des temps d'activités

*Dans la société de l'information les frontières entre les différentes activités ont tendance à disparaître.*

*C'est pourquoi, l'analyse de cette répartition amènera à se poser les questions suivantes : cet équilibre est-il satisfaisant pour moi ? Pour ma famille ? Pour mes proches.*

<sup>9</sup> Ergostressie (du grec ergon - le travail physique et de l'anglais stress - la tension). Le journal « Le Monde initiatives » a présenté le concept d'ergostressie dans son numéro de janvier 2004.

<sup>10</sup> Voir l'accord sur le stress, signé le 8 octobre 2004 par les partenaires sociaux européens, qui doit être négocié en France avant octobre 2007. Le texte de l'accord commenté est téléchargeable sur le site <http://www.ergostressie.com>

## **PARTIE 2 :** **Conception et utilisation des sites intranet et internet syndicaux .**

### **Quelques réflexions sur le SYAM : vers un SYndicalisme à Accès Multiple**

**1 - Les 2 canaux internet : informations "poussées" et informations "tirées"**

**2 - Nécessité de multiplier les canaux : vers le SYAM?**

**3 - Quelques idées pour l'utilisation de la messagerie**

**4 - Quelques idées pour la conception et l'utilisation des sites syndicaux**

**5 - Quelques idées pour l'utilisation du téléchargement**

**6 - Quelques idées pour l'utilisation des forums**

**7 - Les moyens nécessaires**

## **1 - Les 2 canaux d'informations d'internet : informations "poussées" et informations "tirées"**

Un constat: internet et les réseaux remettent en cause l'intermédiation par les possibilités de circuits directs :

- D'une part : les "anciens" intermédiaires doivent redéfinir leurs utilités économiques et sociales.  
Exemples : boutiques commerciales, salle des ventes, agences bancaires, ANPE, APEC, syndicat...
- D'autre part, tout ce que ne fait pas l'"ancien intermédiaire" peut être fait rapidement par un "nouveau"...mais souvent avec moins de compétence.

C'est pourquoi, il est important que les syndicats apprennent à mieux utiliser les possibilités d'internet tant pour les contacts syndicat / salarié que les contacts adhérents / syndicat et militants / syndicat.

En particulier il est important d'avoir en tête que deux canaux principaux sont disponibles sur internet (ou intranet) :

### **- 1 canal d'informations "POUSSÉES" : LA MESSAGERIE**

C'est l'émetteur qui "POUSSE" l'information vers le destinataire à une adresse individuelle connue = (lettre ou tract : voir le paragraphe 3 ci après)

- Cette information ne doit pas être trop fréquente car elle ressemble à un lettre ... ou, si elle n'a pas été sollicitée, à un prospectus publicitaire dans nos boîtes aux lettres. Le SPAM (ou envoi de type publicitaire à un ensemble d'adresses) est une pratique souvent peu goûtée des internautes.
- Cette information doit être très courte.
- Cette information doit comporter peu de pièces jointes (car les gros dossiers doivent être envoyés sous forme " papier " pour éviter les interminables impressions ou accessibles par téléchargement sur le site)

### **- 1 canal d'informations "TIRÉES" : LE SITE WEB (internet ou intranet)**

- C'est le destinataire, c'est à dire l'internaute, qui "TIRE" l'information... s'il le veut.(= panneau d'affichage ).
- Ce site doit séduire l'internaute afin que celui-ci vienne souvent le consulter (voir le paragraphe 4 ci après):
  - Présentation de la qualité d'un journal qui fait apparaître les informations les plus "fraîches"
  - Fréquentes mises à jour.
  - Nombreuses rubriques interactives
  - Nombreux liens avec d'autres sites (notion de réseaux).
  - Il doit servir de " mémoire " comportant tous les éléments utiles accessibles par moteur de recherches interne.

**Il ne faut pas confondre les 2 canaux et il faut apprendre à les utiliser de manière complémentaire : par exemple, on annonce par un message court qu'une information nouvelle se trouve sur le site WEB. C'est ce que font toutes les "Lettres d'informations " des journaux : elles incitent par la messagerie à aller lire une information plus complète sur le site.**

## **2 - Nécessité de multiplier les canaux d'informations: vers le SYAM (Syndicat à Accès Multiple)?**

La diffusion de l'information par les canaux internet ne se substitue pas à la diffusion par les autres canaux : elle est complémentaire.

C'est pourquoi, il est probable que l'on ira de plus en plus vers le SYAM ou le SYndicat à Accès Multiple.

Les canaux "internet" ne sont que des canaux supplémentaires de communication et d'action : ils viennent compléter les autres canaux et non pas se substituer à eux. Il faut s'inspirer de la "banque à accès multiple" pour multiplier les canaux et les adapter à chaque type d'action et de salariés :

- Canal 1 : Contacts "face à face" et échanges d'informations par les délégués syndicaux, les délégués élus, les militants et les adhérents
- Canal 2 : contacts "face à face" et échanges d'informations dans les locaux syndicaux (dans l'entreprise, dans les UD ou les URI)
- Canal 3 : contacts et échanges d'informations par distribution de tracts "papier"
- Canal 4: contacts et diffusion d'informations par le panneau d'affichage
- Canal 5: contacts par téléphone
- Canal 6: diffusion de communiqués de presse et d'interviews
- Canal 7: contacts et échanges d'informations par messagerie intranet et internet
- Canal 8: contacts et échanges d'informations par site intranet et site internet
- canal 9: ....

**Le contact avec les salariés et les adhérents  
et la diffusion d'informations à tous  
doivent profiter des possibilités offertes par internet et intranet :  
mais ces canaux ne remplacent pas les autres types d'échanges.**

**Il faut aller vers le SYAM ou SYndicat à Accès Multiples.**

## **3 - Quelques idées pour l'utilisation de la messagerie**

La réussite de l'utilisation de la messagerie pour l'action collective demande :

- 1- La connaissance des adresses électroniques personnelles des militants et adhérents pour l'envoi d'informations syndicales
- 2 - La connaissance des adresses des salarié(e)s qui acceptent de recevoir des informations syndicales : cela exige la constitution de listes de diffusion (prévoir une inscription possible en cliquant sur un bouton du site Web).
- 3 - La connaissance des structures ou personnalités ou structures extérieures qui acceptent de recevoir des informations syndicales (journalistes, ...).
- 4 - La mise en place d'une fonction permettant la réponse rapides aux messages reçus
- 5 - Le développement du "travail en groupe à distance" ou "travail coopératif" ou ("groupware" en anglais) avec les militants :

- Constitution de communautés d'intérêt (conditions de travail, retraites, ...)
- Structuration : animateur
- Utilisation des techniques d'animation de groupes
- Durée limitée dans le temps

Pour profiter des réseaux, il faut constituer et structurer des "communautés d'intérêts" et connaître les adresses électroniques des militants intéressés.

#### **4 - Quelques idées pour la conception et l'utilisation des sites syndicaux : 20 facteurs importants**

L'objet de ce chapitre n'est pas d'apprendre à concevoir un site Web, mais d'attirer l'attention sur quelques points favorisant la réussite d'un site : il est important de tenir compte de ces 20 facteurs au moment de la conception des sites

##### A - IDENTIFICATION (informations apparentes sur la page d'accueil de l'internaute)

1 - Identification de la structure responsable du site Cette identification (y compris par copyright) est fondamentale

##### B - PAGE D'ACCUEIL et ERGONOMIE

2 - Rapidité d'affichage de la page d'accueil (en octets) : le volume de la page d'accueil (mesuré en octets ou en bits) doit être le plus faible possible afin de permettre aux nombreux internautes qui accèdent à internet par des circuits lents de ne pas attendre trop longtemps l'affichage.

3 - Publics visés par le site : dès la page d'accueil, il faut prévoir plusieurs accès possibles par type de publics.

- Présentation simple pour les non-syndiqués (arborescence intuitive?)
- Présentation simple pour les syndiqués (par secteur d'activités?)
- Présentation simple pour les journalistes (communiqués?)
- Présentation simple pour les étudiants (idéologie syndicale?)
- Présentation pour les étrangers (anglais ou autres...) (Tout site est visité par 20% d'étrangers...)

4 - Facilités de navigation dans le site :

- Sommaire détaillé et plan
- Présence d'un moteur de recherche intégré au site (qui doit apparaître sur la page d'accueil...)
- Programmes complémentaires nécessaires (plugins?)

##### C - PRÉSENTATION GÉNÉRALE ET CONTENU

5 - Nombre de pages du site : la mise en place d'un site est toujours modulaire et progressive. On commence par quelques pages, puis on peut en ajouter au fur et à mesure des besoins et des demandes.

6 - Présentation générale (mise en pages, couleurs,...) : un site doit être aussi bien présenté qu'un journal

7 - Originalités du contenu: il est toujours possible, pour commencer, de prendre des idées sur les autres sites ...

8 - Informations réservées aux adhérents (mot de passe,...?)

9 - Fréquence de mise à jour/ indication de la dernière mise à jour Une mise à jour fréquente multiplie l'utilisation et l'audience du site

**Clés de l'audience d'un site : mise à jour fréquente (on a envie de revenir) et mise en valeur des informations les plus récentes**

## D - INTERACTIVITÉS (possibilités pour les internautes d'envoyer des informations...)

10 - Possibilités simples d'envoyer des messages au site

11 - Possibilités de remplir une demande d'adhésion

12 – Possibilité d'utiliser des logiciels interactifs sur lesquels l'internaute peut agir (Ex : répondre à un sondage, calculer ses impôts, mesurer son temps de travail, évaluer ses conditions de travail et son ergostressie,...)

13 - Possibilités de s'inscrire pour être informé des mises à jour : La "liste de diffusion" multiplie l'utilisation et l'audience du site

14 - Possibilités de télécharger des fichiers à la demande.

15 - Possibilités de participer à des forums de discussion intégrés :LES FORUMS SERONT DE + en + INDISPENSABLES

## E - POPULARITÉ ET REFERENCEMENT SUR LES MOTEURS DE RECHERCHE

16 - Nombre de liens avec d'autres sites : internet est un réseau ; Pour profiter de l' « effet réseau », il faut indiquer sur son propre site de nombreux liens avec les sites "amis" et les sites "intéressants". En particulier tout site syndical doit être un "portail social" donnant les liens "sociaux" et les définitions "sociales" indispensables.

17 - Référencement sur les moteurs de recherche et les annuaires: IL EST INDISPENSABLE DE S'INSCRIRE SUR LES 20 premiers MOTEURS

18 - Publicité sur les autres médias syndicaux : il faut faire la publicité du site SUR TOUS LES AUTRES MEDIA (tracts, papier à lettre, journaux, affiches...)

## F - AUDIENCE (nombre de visites du site et/ou nombre de pages vues)

19 Compteur de visites sur la page d'accueil et sur les pages importantes pour mesurer l'AUDIENCE

20 Nombre d'articles dans la presse parlant du site

**Pour améliorer les taux d'utilité (...et d'audience) des sites syndicaux, il faut :**

**- les rendre plus " interactifs "**

**- les déclarer régulièrement ("référencement") sur les moteurs de recherche**

**- faire de la publicité du site SUR TOUS LES AUTRES MEDIA SYNDICAUX (tracts, papier à lettre, journaux, affiches...)**

**- multiplier les liens avec d'autres sites "amis"(effet "réseau")**

## **5 - Quelques idées pour l'utilisation du téléchargement**

La fonction téléchargement est une fonction très simple, qui permet à l'internaute de recevoir sur son micro-ordinateur, A SA DEMANDE, un fichier mis à sa disposition sur un site Web. Cela évite :

- d'afficher sur le web des informations très longues qui n'intéressent qu'une partie des internautes
- d'envoyer en pièce jointe, par la messagerie, des informations très longues qui n'intéressent qu'une partie des internautes et qui font perdre du temps à l'internaute.

On trouvera un bon exemple d'utilisation du téléchargement sur le site qui permet de prendre connaissance de tous les rapports publics écrits sur les problèmes posés par internet " (<http://www.internet.gouv.fr>)

## **6- Quelques idées pour l'utilisation des forums**

Le forum est une messagerie publique ; chaque internaute peut voir les différents messages envoyés sur le thème du forum : questions et réponses sont ainsi à la disposition de chacun.

La plupart des forums sont "modérés" : un modérateur lit les messages avant de les afficher et vérifie qu'ils correspondent au thème du forum.

La plupart des forums commencent par une liste des "questions les plus fréquemment posées" : cela facilite la participation des internautes au forum.

On trouvera un bon exemple de forum sur le site du " Forum des droits sur l'internet " (<http://www.foruminternet.org/>)

## **7 - Les moyens nécessaires**

Utiliser internet et intranet coûte cher mais c'est un moyen indispensable pour augmenter l'efficacité de l'action syndicale.

- Moyens matériels : micro - ordinateurs + abonnements à une connexion internet + coûts de l'hébergement du site

- Fonctions supplémentaires à prévoir :

Fonction de gestion de la messagerie (réponses aux messages)

Fonction de conception et rédaction du contenu du site

Fonction de réalisation technique et de mise à jour du site

# Annexe 1 :

## Bibliographie et liens

### Généralités

- a) Site internet indispensable à consulter : "*Forum des droits sur l'internet*" (<http://www.foruminternet.org/>)

Le Forum des droits sur l'internet est une association qui réfléchit à l'ensemble des problèmes liés aux évolutions du droit liées au développement de l'utilisation d'internet. En particulier, dans le cadre de cette association, se réunit un groupe de travail sur le thème : " Relations du travail et internet" auquel participe Yves Lasfargue. Mise à jour permanente des textes légaux et forums de discussions très intéressantes. On trouvera sur ce site, très complet, un certain nombre d'accords et de chartes concernant l'utilisation d'intranet et internet. Il est possible aussi de participer aux forums de discussion du "Forum des droits sur l'internet" . Ces forums sont toujours très animés et intéressants.

- b) Un livre indispensable : "*Le droit du travail à l'épreuve des TIC*" - Jean- Emmanuel Ray - Editions Liaisons - Paris - 2001 (2<sup>ème</sup> édition parue en décembre 2001)

Le livre le plus complet et le plus accessible sur le sujet

- c) Une revue de réflexions très complète :

Numéro spécial de la revue "Droit Social" de janvier 2002 sur le thème : "Droit du Travail et Nouvelles Technologies de l'Information et de la Communication"

- d) Nombreux documents CFDT très intéressants :

\* *Site internet de la CFDT Cadres : [www.cadres-plus.net](http://www.cadres-plus.net)*

\* "*Internet/Intranet et droit syndical - Guide d'action syndicale BETOR PUB CFDT*".

Document édité par le BETOR PUB (Fédérations des Services CFDT) : (juin 2000)

Yvan Béraud - 01 42 03 89 55 Courriel : [info@betor-pub.org](mailto:info@betor-pub.org)

\* Action Juridique CFDT : "Protection des salariés et nouvelles technologies" - n°147 - mars 2001

\* « *Intranet : accès et usages arbitraires* » - Magazine Célidé pour les Comités d'Entreprise – n°21 d'août / septembre 2001 ([www.celide.asso.fr](http://www.celide.asso.fr))

- e) Site officiel présentant tous les *textes législatifs français* : <http://www.legifrance.gouv.fr>

Pages de ce site présentant les codes, dont le code du travail, le code civil et le code pénal:

[http://www.legifrance.gouv.fr/html/frame\\_codes1.htm](http://www.legifrance.gouv.fr/html/frame_codes1.htm)

- f) "*DRH et intranets*" : sondage IPSOS pour "Liaisons sociales" et France Télécom, publié dans "Liaisons sociales magazine" de juin 2001

### 1 - Avant le projet : consultation préalable du Comité d'Entreprise

\* "Les experts du Comité d'Entreprise" - guide "Liaisons Sociales" de mars 2000

### 2 - Charte

- Recommandations interministérielles du 19 juin 2001 sur l'utilisation des TIC par les organisations syndicales ( <http://www.fonction-publique.gouv.fr/tic>) dans la fonction publique. Ces recommandations, qui serviront à l'élaboration de chartes ministérielles, visent à permettre aux organisations syndicales de bénéficier des nouvelles technologies pour simplifier leur tâche quotidienne et enrichir le dialogue social. (Voir le texte intégral commenté en annexe 2 –1).

- Exemple de charte sur l'utilisation des TIC (voir le texte intégral commenté en annexe 2 – 2).

### 3/4 - Utilisation par le CE et les organisations syndicales

\* **" Internet/Intranet et droit syndical - Guide d'action syndicale BETOR PUB CFTD "**.

Document édité par le BETOR PUB (Fédérations des Services CFTD) : (juin 2000)

Yvan Béraud - 01 42 03 89 55 Courriel : info@betor-pub.org

\* Exemple d'accord sur l'utilisation d'intranet par les organisations syndicales (Accord France Télécom)  
(Voir le texte intégral commenté en annexe 2 – 3).

## 5 - Libertés et sécurité

Un certain nombre de textes officiels abordent ces problèmes sur le plan mondial, européen, ou français.

- **" Convention européenne des droits de l'homme "** ( <http://www.justice.gouv.fr/textfond/europ1.htm>)

- **"Sécurité des réseaux et de l'information : proposition pour une approche européenne"** -  
Communication de la Commission des Communautés Européennes du 6 juin 2001 (COM(2001) 298final)

- **Avis du Comité Economique et Social européen sur la cyber criminalité** adopté le 12 septembre 2001  
(à l'unanimité des membres du CES européen, y compris les organisations patronales et syndicales  
françaises) sur le rapport de Gérard Dantin (CFTD) disponible au CES

- Avis du Conseil de l'Europe

Pour la France, il faut souligner plusieurs textes importants :

\* **" Cyber surveillance des salariés dans l'entreprise "** - Hubert Bouchet, vice-président délégué de la  
CNIL - mars 2001 - Rapport de la CNIL (Commission Nationale Informatique et Libertés)

\* **"Surveillance et gestion électroniques des salariés : nouveaux risques et nouvel objet de négociation  
au sein du secteur tertiaire"**

ARETE (pour le Projet européen ADAPT et le Ministère de l'emploi et de la solidarité ) - Janvier 1998

ARETE - 3-5 rue de Metz - 75010 Paris - Tel : 01 40 22 12 00 Courriel : contact @arete.fr

\* **"Les libertés publiques et l'emploi"** - Gérard Lyon-Caen - La documentation française - 1991

## 6 - Conditions de travail

\* **« Négocier le télétravail »** - Yves Lasfargue (brochure téléchargeable gratuitement sur le site  
[www.ergostressie.com](http://www.ergostressie.com))

\* **"Halte aux absurdités technologiques"** Yves Lasfargue Editions d'Organisation - 2003

(<http://bullesociale.free.fr>)

\* **« Kit de mesure de la qualité de vie dans la société de l'information »** - Yves Lasfargue (brochure  
téléchargeable gratuitement sur le site [www.ergostressie.com](http://www.ergostressie.com))

\* **"Halte aux absurdités technologiques"** - Yves Lasfargue Editions d'Organisation - Paris - 2003

\* **"Le travail en questions. Enquêtes sur les mutations du travail"** - CFTD - Syros - 2001

\* **"Techno mordus, Techno exclus? Vivre et travailler à l'ère du numérique"**

Yves Lasfargue Editions d'Organisation et Les Echos Paris - 2000

\* **"Télétravail : concilier performance et qualité de vie"**

CEFRIQ - Québec (<http://www.cefrio.qc.ca>) - Mai 2001

\* **"L'État et technologies de l'information et de la communication : vers un service public à accès  
multiple"** Commissariat Général du Plan - Rapport de la mission Lasserre (à laquelle a participé Yves  
Lasfargue) - Documentation Française - mars 2000 ([www.internet.gouv.fr](http://www.internet.gouv.fr))

## 7 - Accords et chartes concernant l'utilisation des TIC : textes commentés (voir annexe 2 et annexe 3)

## **Annexe 2 - 1**

### ***Charte de bon usage des technologies de communication de la "Société INDUSSE"***

Ce document reprend, en le commentant, le texte intégral d'une charte appliquée chez Renault (texte de la charte publiée dans la revue Droit Social de janvier 2002). Nous avons désigné ci -après cette grande entreprise par le pseudo "Société INDUSSE" : cette charte est très complète et aborde de nombreux problèmes.

#### **SOMMAIRE**

INTRODUCTION

CHAPITRE 1ER : STATUT DE LA CHARTE

- 1 - 1 OBJET DE LA CHARTE
- 1 - 2 CHAMP D'APPLICATION DE LA CHARTE
- 1 - 3 APPLICATION DE LA CHARTE.
- 1 - 4 SANCTIONS

CHAPITRE 2 : RÈGLES D'UTILISATION DES RESSOURCES

- 2 - 1 RÈGLES GÉNÉRALES
- 2 - 2 MESURES DE SÉCURITÉ
- 2 - 3 MATÉRIELS, PROGRAMMES, LOGICIELS, ETC.
- 2 - 4 VIRUS INFORMATIQUES
- 2 - 5 MESSAGERIE ÉLECTRONIQUE
- 2 - 6 INTERNET
- 2 - 7 FORUMS DE DISCUSSION
- 2 - 8 INFORMATIONS, DONNÉES ET FICHIERS
- 2 - 9 VIGILANCE.

CHAPITRE 3 : FORMATION

CHAPITRE 4 : AUDITS

CHAPITRE 5 : ENTRÉE EN VIGUEUR

CHAPITRE 6 : PUBLICITÉ

#### **INTRODUCTION**

La société INDUSSE met à la disposition de tout utilisateur des équipements informatiques (PC, stations, logiciels, etc.), des moyens de communication (messageries, accès internet, « assistants personnels numériques », etc.), ainsi que des informations et données (bases de données, images, vidéos, etc. ), qui sont nécessaires à l'accomplissement de sa mission.

Est considéré comme « utilisateur » toute personne, quel que soit son statut (salarié, personnel intérimaire, stagiaire, consultant, partenaire, etc.), qui est amenée à créer, consulter et mettre en œuvre ces ressources.

L'utilisation de ces ressources doit être uniquement professionnelle, sauf exception prévue dans la présente charte, et tournée vers la performance de la société et la satisfaction des clients.

La présente charte ne fait pas obstacle à ce que des dispositions spécifiques soient définies par l'entreprise en vue d'une utilisation des ressources informatiques, électroniques et numériques par les représentants du personnel. .

Ces ressources font partie du patrimoine de la société INDUSSE. A cet égard, toute information émise, reçue ou stockée sur le poste de travail et les moyens de communication mis à sa disposition est et demeure la propriété de l'Entreprise.

Chaque utilisateur doit être conscient que, d'une part, l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et du code de déontologie de INDUSSE, dans le respect aussi de la sécurité de l'Entreprise et du bon usage, gage d'efficacité opérationnelle, et que, d'autre part, sa négligence ou sa mauvaise utilisation des ressources fait encourir des risques à l'ensemble de l'Entreprise, et donc à lui-même.

La société INDUSSE définit et met en œuvre les moyens appropriés, en l'état de la technique, pour protéger les utilisateurs et pour protéger les ressources mises à leur disposition contre tout risque de destruction ou d'altération.

L'Entreprise prend donc les engagements suivants :

1. Se donner les moyens budgétaires, humains, techniques, afin de respecter cette Charte, dans le cadre des contrats internes de service.
2. Définir un « Plan de continuité de service » pour toute application sensible.
3. Garantir un archivage des données déterminé conformément à la législation applicable en matière de conservation des informations et aux prescriptions de la société INDUSSE.
4. Acquérir les droits d'usage ou de propriété intellectuelle nécessaires à l'utilisation de ces ressources dans le cadre professionnel évoqué ci-dessus.

#### ***Commentaires sur l'introduction et les technologies concernées***

*Il s'agit d'une charte rédigée par l'entreprise et non d'un accord négocié et signé par les organisations syndicales. Cette charte a été soumise pour avis aux comités d'entreprise et aux comités d'établissement concernés (voir chapitre 5).*

*Cette charte ne concerne pas seulement internet et intranet : elle concerne l'utilisation de l'ensemble des ressources informatiques, électroniques et numériques.*

*Cette charte n'est pas un modèle, mais elle peut servir d'exemple pour les autres entreprises.*

## **CHAPITRE 1ER : STATUT DE LA CHARTE**

### **1 - 1 OBJET DE LA CHARTE**

La présente Charte a pour vocation d'exposer les principales règles et précautions que tout utilisateur doit respecter et mettre en œuvre

### **1 - 2 CHAMP D'APPLICATION DE LA CHARTE**

La Charte concerne la totalité des utilisateurs. A ce titre, elle doit être communiquée à tout utilisateur, interne ou extérieur à l'Entreprise.

La Charte est diffusée à l'ensemble du personnel de la société et mise à disposition sur l'intranet INDUSSE. Il y est fait référence dans le règlement intérieur de chaque site.

Les contrats entre INDUSSE et tout tiers donnant accès aux données, aux programmes informatiques ou autres moyens de l'Entreprise, devront stipuler que les utilisateurs s'engagent à respecter la présente Charte. Les responsables des utilisateurs extérieurs s'engagent à faire respecter la présente Charte par leurs propres salariés et éventuelles entreprises sous-traitantes.

#### ***Commentaires sur le champ d'application***

*Cette charte concerne tous les salarié(e)s, mais aussi les utilisateurs extérieurs à l'entreprise*

### **1 - 3 APPLICATION DE LA CHARTE**

En qualité d'utilisateur des ressources de l'Entreprise, chaque utilisateur s'engage à connaître et à appliquer l'ensemble des dispositions de la présente Charte.

L'entreprise s'engage, pour sa part, à mettre en œuvre tous les moyens pertinents, compte tenu de l'état des techniques, afin de garantir la meilleure sécurité possible des installations mises à la disposition des utilisateurs.

## 1 - 4 SANCTIONS

Le non respect des règles et mesures de sécurité figurant dans la présente Charte engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose éventuellement et de manière appropriée et proportionnée au manquement commis, aux sanctions disciplinaires définies par le règlement intérieur de chaque site.

## CHAPITRE 2 : RÈGLES D'UTILISATION DES RESSOURCES

### 2 - 1 RÈGLES GÉNÉRALES

L'utilisateur est responsable de l'usage qu'il fait des ressources de l'Entreprise dans l'exercice de sa fonction au sein de la société INDUSSE.

Il doit réserver l'usage de ces ressources au cadre de son activité professionnelle. Un usage personnel des moyens de communication est toutefois exceptionnellement admis pour répondre à des situations d'urgence.

#### *Commentaires sur la possibilité d'usage personnel*

*"Un usage personnel des moyens de communication est toutefois exceptionnellement admis pour répondre à des situations d'urgence. " : cet article est important car il autorise des pratiques souvent interdites.*

Par conséquent, il ne doit se livrer, en aucune circonstance, à l'une quelconque des activités suivantes :

- Charger, stocker, publier, diffuser ou distribuer, au moyen des ressources de l'Entreprise, des documents, informations, images, vidéos, etc. :
  - à caractère violent, pornographique ou contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs, de caractère diffamatoire et de manière générale illicite,
  - portant atteinte aux ressources de l'Entreprise et plus particulièrement à l'intégrité et à la conservation des données de l'Entreprise,
  - portant atteinte à l'image de marque interne et externe de la société INDUSSE.

Il est interdit d'accéder à des serveurs Web traitant de ces sujets avec le risque de voir l'adresse e-mail de l'utilisateur reprise dans un courrier de masse comportant des pièces jointes illicites. Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt.

L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc. .

- Utiliser les ressources de l'Entreprise à des fins de harcèlement, menace ou d'injure et de manière générale violer des droits en vigueur.
- Charger, stocker ou transmettre des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle, sauf à posséder les autorisations nécessaires. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels fichiers
- Charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, etc., qui sont protégés par les lois sur la propriété intellectuelle, autres que ceux qui sont expressément autorisés par l'Entreprise. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes, logiciels, progiciels, etc.
- Utiliser les matériels, programmes, logiciels, progiciels, etc., mis à sa disposition par l'Entreprise, en violation des lois sur la propriété intellectuelle, des règles techniques applicables et des prescriptions définies par l'Entreprise.
- Charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées.
- Falsifier la source d'éléments contenus dans un fichier

- Envoyer des messages en masse (plus de 20 destinataires, hors diffusion sur des listes de l'Entreprise pour raisons de service) ou en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement).
- Utiliser les ressources de l'Entreprise de manière à gêner l'accès des autres utilisateurs.

Pour rappel, certaines des activités énoncées ci-dessus peuvent constituer des infractions de nature pénale.

L'Entreprise se réserve la possibilité d'effectuer des vérifications et contrôles réguliers, dans les limites prévues par la loi.

#### ***Commentaires sur les interdictions***

*Cette liste mélange des activités interdites par la loi, et des règles permettant un bon fonctionnement de l'entreprise. Il faut remarquer que, dans cette entreprise, "l'envoi de messages en masse " commence à 20 destinataires.*

## **2 - 2 MESURES DE SÉCURITÉ**

Afin de permettre la mise en œuvre par l'entreprise d'une parade de premier niveau, l'utilisateur doit respecter au minimum les prescriptions suivantes :

**Prescription 1 :** Mettre toujours un mot de passe quand il lui est demandé.

**Prescription 2 :** Changer de mot de passe régulièrement.

**Prescription 3 :** Ne jamais prêter son identifiant/mot de passe.

**Prescription 4 :** Protéger spécifiquement ses fichiers confidentiels/secret INDUSSE.

**Prescription 5 :** Utiliser un anti-virus sur tout document de provenance externe à l'entreprise.

**Prescription 6 :** Ne pas répondre aux messages en masse ou en chaîne des messageries.

**Prescription 7 :** Éteindre son poste par arrêt logiciel et non par l'interrupteur pour terminer proprement ses sessions (hors cas de blocage technique).

**Prescription 8 :** Ne jamais quitter son poste de travail en laissant accessible une session en cours (mise en veille avec mot de passe après 5 minutes d'inactivité).

**Prescription 9 :** Ne pas laisser à disposition des supports informatiques (disquette, cassette, CDROM,...) contenant des données confidentielles, dans un bureau ouvert.

**Prescription 10 :** Ne pas oublier de récupérer, sur les fax, imprimantes ou photocopieurs, les documents sensibles que l'on envoie, imprime ou photocopie.

L'absence de respect des prescriptions ci dessus ne pourra être sanctionnée, conformément au point 4 du chapitre 1 er de la présente charte, que si les manquements observés ont nui ou sont susceptibles de nuire à l'entreprise ou aux personnes qui s'y trouvent, ou ont été réitérés en dépit de mises en garde.

#### ***Commentaires sur la sécurité***

*L'un des premiers objectifs de toute charte concernant l'utilisation des TIC est la protection de la sécurité des données et du fonctionnement de l'entreprise. C'est pour cela que des sanctions sont prévues.*

## **2 - 3 MATÉRIELS, PROGRAMMES, LOGICIELS, ETC.**

L'Entreprise met à la disposition de l'utilisateur des ressources (PC, stations, serveurs « assistants personnels numériques », téléphones multifonctions, fax, etc.) pour exercer son activité professionnelle conformes aux règles juridiques et techniques applicables et aux prescriptions définies par l'Entreprise (standards). L'utilisateur s'interdit par conséquent de modifier ces standards, notamment par l'ajout de logiciels hors standards pour lesquels l'Entreprise pourrait être accusée de piratage, en dehors d'incompatibilités potentielles. A des fins de précaution, certaines configurations peuvent être verrouillées par l'Entreprise (poste de travail, etc.).

Le disque dur du poste de travail de l'utilisateur ne doit pas contenir de programmes, logiciels, documents, fichiers, informations ou données, tels que rappelés ci-dessus, et notamment des fichiers à caractère pornographique, nazi ou raciste ainsi que tout autre fichier prohibé par la loi locale.

Les utilisateurs de postes portables s'engagent, quel que soit l'endroit où ils se trouvent, à sécuriser leur matériel et l'accès aux données qu'il contient. L'utilisateur ne doit jamais transporter l'intégralité de fichiers qui auraient une valeur stratégique pour la société INDUSSE. Les informations et données sensibles stockées sur le disque dur de son poste portable devront être chiffrées conformément aux directives données par la direction ou l'entreprise dont relève l'utilisateur. Un outil de chiffrement est mis à la disposition des utilisateurs à cet effet.

#### ***Commentaires sur la sécurité des portables***

*La charte insiste sur les précautions que doivent prendre les utilisateurs de micro-ordinateurs portables, points faibles de la sécurité du réseau..*

Les ressources mises à la disposition de tout utilisateur, et notamment les disques durs, pourront faire l'objet de vérifications et de contrôles par l'Entreprise, dans les limites prévues par la loi.

#### ***Commentaires sur le contrôle des disques durs***

*Il faut rappeler que ces vérifications et contrôles sont désormais limitées par l'arrêt de la Cour de cassation du 2 octobre 2001 concernant le respect d'une zone de "vie privée" dans les lieux et temps professionnels. Voir annexe 2 – 4.*

*Voir aussi la fiche 5 sur le respect des libertés.*

## **2 - 4 VIRUS INFORMATIQUES**

Le poste de travail (station, micros, portable, etc.) de chaque utilisateur est en règle générale équipé d'un logiciel anti-virus.

Cependant, l'utilisation des applications communicantes (internet, messagerie, etc.) et des supports de stockage (disquette, CD-Rom), peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'utilisateur, à l'insu de ce dernier, de programmes ou fichiers, qui altèrent ou pillent les données et logiciels qu'il contient.

En cas d'anomalie, l'utilisateur doit stopper toute transaction et prévenir immédiatement le Service de dépannage informatique.

## **2 - 5 MESSAGERIE ÉLECTRONIQUE**

L'utilisation des outils de messagerie électronique est réservée à un usage strictement professionnel sauf exception visée au point 1 du chapitre 2 de la présente charte.

Toute utilisation à des fins promotionnelles est interdite.

L'utilisateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie, etc.), car le message électronique peut :

- être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant;
- constituer une preuve ou un commencement de preuve par écrit.

De même que partout ailleurs, la courtoisie constitue une règle de base dans tous les échanges électroniques.

Par ailleurs, l'utilisateur doit rédiger des messages courts et clairs afin d'éviter toute surcharge informationnelle nuisant à l'efficacité de la communication. Il doit également utiliser avec discernement les listes de diffusion personnelles ou collectives. Il doit éviter l'envoi de copies à un nombre injustifié de destinataires.

#### ***Commentaires sur la gestion des volumes de messagerie***

*La charte essaie de limiter les volumes échangés par messagerie électronique... avec des conseils de "bon sens" du type "messages courts" ou "nombre injustifié de destinataires"*

Enfin, il est rappelé que les messages électroniques envoyés d'une entité de la société INDUSSE à une autre entité de la société INDUSSE sont, en général, considérés comme sécurisés. Dans la plupart des autres cas, les messages électroniques transitent par le Web et peuvent donc, à tout moment, être interceptés, visualisés, enregistrés et utilisés à d'autres fins par un tiers.

## 2 - 6 INTERNET

L'Internet est un outil qui est mis à la disposition de l'utilisateur à titre professionnel sauf exception visée au point 1 du chapitre 2 de la présente charte. Il doit donc en faire un usage approprié.

L'accès à Internet est attribué individuellement à chaque utilisateur, afin de lui permettre de visiter, à des fins professionnelles, les sites du monde entier sous le nom de l'Entreprise. Toutefois, lorsqu'il « navigue » sur le Web, l'identifiant de l'utilisateur (qui apparaît sous le nom de « INDUSSE » sur les sites informatiques extérieurs) ainsi que les sites visités sont enregistrés dans les limites prévues par la loi.

En outre, chaque site internet pouvant être régi par des règles juridiques autres que le droit français, toutes précautions doivent être prises à cet égard par l'utilisateur.

Par ailleurs, toutes les activités de l'utilisateur ainsi que les données concernant l'utilisateur (sites consultés, messages échangés, données fournies à travers des formulaires, données collectées à l'insu de l'utilisateur, etc.) peuvent être enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations de l'Entreprise, etc., et utilisées à des fins commerciales ou autres. Toutes précautions doivent également être prises par l'utilisateur à cet égard.

### ***Commentaires sur la "transparence" d'internet : ne soyons ni naïfs, ni paranoïaques !!***

*La charte rappelle que toutes les activités de l'utilisateur peuvent être enregistrées et analysées sur ... internet. Il est bon que chaque utilisateur se rappelle que ce qui est vrai pour internet est aussi vrai pour intranet.*

*Ne soyons pas naïfs et soyons lucides sur les caractéristiques de l'utilisation des réseaux: toute utilisation des TIC est totalement transparente. Mais ce n'est pas une raison pour avoir peur...*

A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet est sujet à une supervision et à des vérifications et audits réguliers par l'Entreprise, dans les limites prévues par la loi.

### ***Commentaires sur les statistiques et la confidentialité***

*Soyons lucides : pour des raisons statistiques, l'entreprise vérifie tous les flux (mais pas tous les contenus). L'important est que ces informations ne soient pas utilisées à d'autres fins que l'audit technique.*

*Il est bon de se rappeler l'engagement pris par les recommandations interministérielles du 19 juin 2001:*

*"L'administration s'engage à respecter la confidentialité des messages électroniques en provenance ou à destination des boîtes aux lettres syndicales (contenu, auteurs et destinataires), du contenu des listes de diffusion élaborées par les organisations syndicales et de l'identité des auteurs des messages destinés à un forum de discussion modéré par une organisation syndicale lorsque l'anonymat des participants a été décidé d'un commun accord entre l'administration et les syndicats."  
" (article 1.3)*

*On peut noter aussi l'accord France Télécom qui prévoit (article 1): "France Télécom s'engage, dans le cadre du respect de la liberté individuelle, à ne pas rechercher l'identification des salariés consultant le ou les sites syndicaux( art. 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)."  
Voir l'annexe 2 – 3.*

## 2 - 7 FORUMS DE DISCUSSION

Les forums de discussions répondent aux mêmes règles de bon usage que la messagerie électronique. En outre, le sens de la responsabilité de chacun conduit à ne pas se permettre de participer anonymement à ces discussions électroniques.

## **2 - 8 INFORMATIONS, DONNÉES ET FICHIERS**

L'Entreprise est responsable de :

- La mise à disposition de ressources sécurisées conformes aux règles juridiques et techniques applicables et aux prescriptions définies par l'entreprise (standards).
- La maintenance technique des ressources et de leur sécurisation.

L'utilisateur est responsable de la pérennité de ses fichiers, données, informations, etc., ainsi que des accès de lecture et de modification qu'il peut donner à d'autres personnes ou Utilisateurs.

## **2 - 9 VIGILANCE**

Il est demandé à chaque utilisateur de signaler toute tentative de violation de son poste de travail ou de ses fichiers ou données, dès qu'il en a connaissance, auprès de son Responsable Sécurité des Systèmes Informatiques local (Administrateur Système des Systèmes Informatiques) afin de pouvoir apprécier l'imputabilité personnelle des incidents qui pourraient survenir.

## **CHAPITRE 3 : FORMATION**

L'entreprise organise les formations nécessaires à chaque utilisateur pour appliquer les règles et prescriptions de sécurité prévues par la présente charte.

Elles comprennent notamment:

- une formation en ligne sur la sécurisation du poste de travail et l'accès aux applications / services INDUSSE, (mise en place, changement des mots de passe, perte des mots de passe)
- un rappel en ligne des procédures de demandes d'accès aux applications / services INDUSSE

Une formation spécifique adaptée accompagne l'évolution des postes de travail.

Chaque utilisateur doit se former aux techniques de sécurité, et maintenir son niveau de connaissance en fonction de l'évolution de ces techniques.

## **CHAPITRE 4 : AUDITS**

La société pourra procéder périodiquement, par tous moyens, à des audits de contrôle de la bonne application de la présente Charte, dans les limites prévues par la loi.

### ***Commentaires sur les audits***

*Il faut rappeler que ces audits de contrôles sont désormais limités par l'arrêt de la Cour de cassation du 2 octobre 2001 concernant le respect d'une zone de "vie privée" dans les lieux et temps professionnels.  
Voir aussi la fiche 5 sur le respect des libertés.*

## **CHAPITRE 5 : ENTRÉE EN VIGUEUR**

La présente charte a été soumise pour avis aux comités d'entreprise et aux comités d'établissement concernés. Elle s'applique, les formalités requises achevées, à partir de 2001.

### ***Commentaires sur l'avis du Comité d'entreprise***

*Toute charte comportant des droits, des devoirs et des sanctions doit être soumise au Comité d'entreprise, comme toutes les modifications du règlement intérieur.*

## CHAPITRE 6 : PUBLICITÉ

Les utilisateurs seront informés du contenu de la présente Charte.

### *Commentaires sur la publicité*

*Dans certaine entreprise l'entreprise demande à chaque salarié(e) de signer personnellement la charte. Cette signature est souvent une manière de faire accepter un certain nombre de systèmes de contrôles individualisés afin que l'entreprise ne puisse être accusée de "contrôler les salariés à leur insu" (article L 121 - 8 du Code du travail).*

### *Article L121- 8 du Code du travail*

*Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.*

*Voir aussi la fiche 5 sur le respect des libertés*

## Annexe 2 - 2

### ***Recommandations interministérielles sur l'utilisation des TIC par les organisations syndicales dans les fonctions publiques (19 juin 2001)***

Extraits du communiqué de presse du 19 juin 2001 diffusé par le ministère de la fonction publique et de la réforme de l'État

Michel SAPIN, ministre de la fonction publique et de la réforme de l'État, a présidé le mardi 19 juin 2001 la Commission permanente de modernisation des services publics composée de représentants de l'administration, des organisations syndicales et des usagers. Lors de cette réunion, plusieurs mesures relatives à l'utilisation par l'administration des technologies de l'information et de la communication ont été décidées.

- La commission de modernisation a approuvé des recommandations interministérielles sur l'utilisation des TIC par les organisations syndicales. Ces recommandations, qui serviront à l'élaboration de chartes ministérielles, visent à permettre aux organisations syndicales de bénéficier des nouvelles technologies pour simplifier leur tâche quotidienne et enrichir le dialogue social.

.....

#### A. Faire entrer le dialogue social dans la société de l'information

Les intranets et la messagerie se généralisent dans les services publics. Leur utilisation au service du dialogue social est donc de plus en plus fréquente. Plusieurs ministères et administrations ont déjà signé des accords sur ce sujet avec les organisations syndicales (ministères de l'économie, des finances et de l'industrie, de l'intérieur, services du Premier ministre, caisse des dépôts, etc.).

Afin d'accompagner et d'accélérer ce mouvement, le ministère de la fonction publique et de la réforme de l'État rend publiques aujourd'hui des recommandations pour la réalisation de chartes ministérielles sur l'utilisation des technologies de l'information et de la communication par les organisations syndicales. Cette utilisation vise à simplifier la tâche quotidienne des acteurs du dialogue social pour qu'elle soit plus efficace.

Ce document est le résultat d'une négociation très constructive entre organisations syndicales et administrations, au sein du groupe sur l'utilisation des technologies de l'information et de la communication dans l'administration, issu de la commission de modernisation des services publics.

Les recommandations portent sur les modalités d'utilisation par les organisations syndicales :

- des messageries électroniques internes à l'administration ;
- des intranets administratifs ;
- des forums de discussion sur ces intranets.

Ces recommandations interministérielles ont vocation à être déclinées par chaque département ministériel en fonction de l'architecture technique de son réseau, des demandes exprimées par les organisations syndicales qui y sont implantées et en tenant compte d'une nécessaire période d'expérimentation.

Ces recommandations prévoient notamment l'équipement des locaux syndicaux en matériel et logiciels. Il s'effectuera au rythme moyen de l'équipement professionnel des agents affectés dans le service au titre duquel les locaux syndicaux sont attribués. Ils permettront la connexion gratuite au réseau interne du service et/ou du département ministériel concerné (messagerie et intranet). L'administration prendra à sa charge la formation des membres des syndicats à l'utilisation des nouveaux outils informatiques mis à leur disposition.

Des boîtes aux lettres aux coordonnées des syndicats seront ouvertes sur les postes des locaux syndicaux, sur les postes extérieurs autorisés à être reliés au réseau ministériel ou encore sur les postes professionnels des responsables syndicaux. Ces boîtes aux lettres ont vocation à être utilisées pour la vie interne des

syndicats, notamment la correspondance avec les adhérents et les sympathisants. Enfin, si les chartes ministérielles le prévoient, ces boîtes pourront servir pour des envois à l'ensemble des agents d'un service.  
(<http://www.iinternet.gouv.fr>)  
( <http://www.fonction-publique.gouv.fr/tic>)

---

# PROJET DE RECOMMANDATIONS POUR LA RÉALISATION D'UNE CHARTE MINISTÉRIELLE SUR L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION PAR LES ORGANISATIONS SYNDICALES (texte intégral du 19 juin 2001)

## Remarques préliminaires

Dans le cadre de l'introduction généralisée des nouvelles technologies de l'information et de la communication dans les services de l'État, il est nécessaire et naturel d'associer les organisations représentant le personnel à la réflexion sur les conséquences que ces nouveaux instruments peuvent avoir sur l'organisation des services. Parallèlement, il convient de les faire bénéficier d'un large accès, pour leurs propres besoins, aux nouveaux instruments de travail de l'administration. Ces nouveaux moyens ne se substituent pas à ceux qui sont prévus par le décret n° 82-447 du 28 mai 1982 relatif à l'exercice du droit syndical dans la fonction publique.

Les recommandations qui suivent concernent ainsi les modalités d'utilisation par les organisations syndicales :

- des messageries électroniques internes à l'administration ;
- des intranets administratifs ;
- des forums de discussion sur ces intranets.

Les conditions d'utilisation des nouvelles technologies par les organisations syndicales, préconisées dans le présent document, visent à simplifier l'action quotidienne des acteurs du dialogue social pour qu'elle soit efficace, tout en préservant le bon fonctionnement de l'outil de travail, propriété de l'administration.

Ces recommandations interministérielles ont vocation à être déclinées par chaque département ministériel (et, éventuellement, par chaque service en son sein ainsi que par les établissements publics nationaux et les autres institutions administratives employant des agents publics relevant du titre II du statut général des fonctionnaires), en fonction de l'architecture de son réseau, des demandes exprimées par les organisations syndicales qui y sont implantées et en tenant compte d'une nécessaire période d'expérimentation.

Elles ont donc pour objectif de servir de guide à la rédaction de chartes ministérielles sur l'utilisation des technologies de l'information et de la communication par les organisations syndicales, comme plusieurs ministères ou établissements en ont déjà réalisé. Ces chartes peuvent prendre la forme d'un protocole d'accord entre l'administration et les syndicats représentés en son sein ou être précédées d'un tel protocole. Elles pourront s'inscrire dans le cadre des dispositions qui précisent les conditions générales d'utilisation des nouvelles technologies au sein de chaque ministère - lorsqu'elles existent - et qui portent, par exemple, sur les consignes de sécurité à respecter dans l'usage des nouveaux instruments de travail. Les chartes ministérielles résultant de ce travail pourront comporter une clause de révision, afin de mettre régulièrement en adéquation leur contenu avec la réalité technique locale.

### *Commentaires du texte préliminaire*

*Ces recommandations sont un guide qui doit servir à la rédaction de chartes ministérielles opérationnelles.*

*Afin de lever l'ambiguïté sur le sens du mot charte (qui en général un document non signé par les organisations syndicales), il est précisé que "ces chartes peuvent prendre la forme d'un protocole d'accord entre l'administration et les syndicats représentés en son sein ou être précédées d'un tel protocole."*

*L'important est de suivre l'établissement de ces chartes encore peu nombreuses (ministères de l'économie, des finances et de l'Industrie, de l'intérieur, services du Premier ministre, caisse des dépôts, etc.)*

## **1. RECOMMANDATIONS GENERALES**

### **1.1 Détermination des organisations syndicales bénéficiant d'un accès aux technologies de l'information et de la communication.**

Chaque département ministériel déterminera les organisations syndicales bénéficiant des facilités décrites ci-dessous, selon l'architecture de son réseau, ses contraintes de sécurité spécifiques et en tenant compte du principe jurisprudentiel de concordance.

En période électorale, c'est à dire à compter de la date de clôture du dépôt des candidatures jusqu'au jour du scrutin inclus, l'accès aux technologies de l'information et de la communication devra être assuré, dans des conditions comparables, à l'ensemble des organisations syndicales admises à présenter des candidats dans le même champ organisationnel.

### **1.2. Mise à disposition de matériel informatique**

L'équipement des locaux syndicaux en matériel et logiciels informatiques s'effectuera au rythme moyen et selon les mêmes modalités, notamment en termes de sécurité, que l'équipement professionnel des agents affectés dans le service au titre duquel les locaux syndicaux sont attribués. Ces dispositions concernent les locaux mis à la disposition des organisations syndicales par l'administration en vertu de l'article 3 du 14 décret n° 82-447 du 28 mai 1982. Le matériel et les logiciels fournis permettront la connexion gratuite au réseau interne du service et/ou du département ministériel concerné (messagerie et intranet), un accès à l'internet lorsque la configuration du réseau de l'administration le permet ainsi que la mise en ligne d'informations destinées aux sites syndicaux hébergés sur l'intranet.

Dans ce cadre, les organisations syndicales disposant d'un accès à un local propre bénéficient toutes du même rythme d'équipement. Celles qui disposent d'un local partagé bénéficient d'un équipement collectif.

Dans le cas des services où un grand nombre d'agents accède régulièrement de façon externe au réseau ministériel (par exemple, ministère de l'éducation nationale), il peut être envisagé, si le niveau de sécurité informatique défini pour ce réseau le permet, que des ordinateurs privés accèdent aux services utiles de celui-ci. Cette hypothèse concerne les cas où le branchement des locaux syndicaux, mis à disposition par l'administration, ou bien la mise à disposition de matériel au bénéfice des responsables syndicaux pour leurs besoins professionnels ne suffiraient pas à offrir un accès aux nouvelles technologies à tous les syndicats qui doivent en bénéficier.

Par ailleurs, pour des raisons pratiques (en particulier, répartition quasi impossible des créneaux d'utilisation et confidentialité des fichiers informatiques de l'administration contenus dans l'ordinateur concerné), l'accès aux nouvelles technologies par les organisations syndicales sera négocié au cas par cas lorsqu'il n'existe qu'un seul poste branché au réseau ministériel au sein d'un service local. L'administration prendra à sa charge la formation des membres des syndicats à l'utilisation des nouveaux outils informatiques mis à leur disposition. Cette formation pourra également faire l'objet de congés pour la formation syndicale.

#### *Commentaires du texte concernant les moyens*

*Les moyens prévus (locaux, matériels, formation) semblent intéressants et complets: reste à savoir ce que donneront ces principes au moment de la réalisation sur le terrain.*

### **1.3. Confidentialité des échanges syndicaux**

L'administration s'engage à respecter la confidentialité des messages électroniques en provenance ou à destination des boîtes aux lettres syndicales (contenu, auteurs et destinataires), du contenu des listes de diffusion élaborées par les organisations syndicales et de l'identité des auteurs des messages destinés à un forum de discussion modéré par une organisation syndicale lorsque l'anonymat des participants a été décidé d'un commun accord entre l'administration et les syndicats.

Elle peut apporter son aide aux organisations syndicales pour faire respecter la confidentialité des données citées ci-dessus à l'égard de tiers. Elle ne peut être tenue pour responsable des violations qui seraient, cependant, commises par des tiers.

Les conditions techniques de cette aide font l'objet d'une concertation avec les organisations syndicales. Dans ce cadre, l'administration peut, par exemple, mettre à la disposition des organisations syndicales les moyens qu'elle emploie pour assurer la sûreté de ses propres contenus.

### *Commentaires du texte concernant la confidentialité*

*Cet article est très intéressant : la confidentialité concerne non seulement le contenu, mais aussi les auteurs et les destinataires.*

*Ce texte pourrait servir de base à certains accords d'entreprise*

#### **1.4. Responsabilité des organisations syndicales et de leurs membres**

L'affichage virtuel et la modération des forums de discussion étant effectués par les organisations syndicales, celles-ci, ainsi que leurs membres, engagent leur responsabilité sur les informations ou prises de position qu'ils décident de rendre publiques.

C'est en particulier le cas dans l'hypothèse du non-respect de dispositions de nature pénale (par exemple, injure et diffamation publiques, contrefaçon, obligations imposées par la loi Informatique et libertés) ou statutaires (par exemple, violation du devoir de discrétion professionnelle ou de l'obligation de réserve).

### *Commentaires du texte concernant les responsabilités éditoriales*

*La responsabilité des organisations syndicales est clairement définie.*

*Ce texte aussi pourrait servir de base à certains accords d'entreprise*

## **2. MESSAGERIE INTERNE**

Il sera attribué des boîtes aux lettres aux coordonnées des syndicats (sur les postes des locaux syndicaux ou sur les postes extérieurs autorisés à être reliés au réseau ministériel dans les conditions décrites au 1.2 ou, encore, sur les postes professionnels des responsables syndicaux). Seules ces boîtes serviront pour l'envoi de messages à contenu syndical. Elles ne se substituent pas aux boîtes professionnelles des responsables syndicaux.

Les chartes ministérielles prévoient des règles de bon comportement dans l'usage de la messagerie, élaborées par l'administration en concertation avec les organisations syndicales et pouvant s'inscrire dans le cadre des chartes générales d'utilisation des nouvelles technologies évoquées dans les remarques préliminaires.

Les boîtes aux lettres ont vocation à être utilisées prioritairement pour la vie interne des syndicats, notamment pour la correspondance avec les adhérents et les sympathisants.

Pour ce faire, les organisations syndicales établissent, sous leur seule responsabilité, des listes de diffusion avec l'accord préalable des agents concernés. Cet accord est présumé pour les adhérents. Les autres agents s'inscrivent sur les listes de diffusion à partir des sites syndicaux hébergés sur l'intranet administratif. Les agents figurant sur ces listes peuvent demander à tout moment à en être radiés. Les organisations syndicales sont tenues de faire droit à ces demandes.

### *Commentaires du texte concernant les listes de diffusion*

*Les organisations syndicales peuvent créer des listes de diffusion, comprenant leurs adhérents + les agents ayant donné leur adresse en s'inscrivant sur la liste.*

*C'est une disposition originale, très favorable aux organisations syndicales, car l'utilisation des listes de diffusion est interdite dans tous les accords d'entreprise.*

Par ailleurs, les boîtes peuvent éventuellement servir pour des envois à l'ensemble des agents d'un service. Cependant, l'information syndicale à caractère général a vocation à être portée à la connaissance des agents prioritairement par le biais des sites sur l'intranet.

Dans le cas où les envois généraux seraient autorisés, les règles de bon comportement mentionnées ci-dessus définissent les conditions dans lesquelles de tels messages seront diffusés. Pour éviter la saturation des réseaux, elles peuvent notamment prévoir que ces messages seront diffusés par le biais de relais locaux et 16 elles fixent

un nombre de messages de ce type pouvant être émis par période donnée, leur taille maximale, l'existence ou non de pièces jointes, les horaires d'envoi... Dans les administrations où les agents ne peuvent pas paramétrer leur boîte à lettres pour refuser les messages de certains émetteurs, ils peuvent alors demander à tout moment à ne plus recevoir de messages résultant d'un envoi général. Les organisations syndicales sont tenues de faire droit à ces demandes.

#### ***Commentaires du texte autorisant le "SPAM"***

*"Les boîtes peuvent éventuellement servir pour des envois à l'ensemble des agents d'un service." : cela veut dire que le "SPAM" (envoi de type publicitaire) est autorisé. C'est une aussi disposition originale, très favorable aux organisations syndicales, car l'utilisation des forums est interdite dans tous les accords d'entreprise. Mais ... il est possible aux agents de refuser les messages syndicaux.*

L'interpellation des responsables hiérarchiques par le biais de messages électroniques identiques envoyés en nombre (pétition électronique) n'est pas autorisée.

Le non respect des modalités d'utilisation peut conduire à la fermeture des boîtes aux lettres concernées par l'administration, dans les conditions définies par chaque ministère en concertation avec les organisations syndicales.

#### ***Commentaires du texte concernant les sanctions***

*Les "pétitions" sont interdites  
Sanctions prévues : la fermeture des boîtes aux lettres.*

### **3. SITES DES ORGANISATIONS SYNDICALES SUR LES INTRANETS ADMINISTRATIFS**

Il sera attribué aux syndicats un espace sur l'intranet correspondant au champ dans lequel ils sont implantés, avec possibilité de renvois (liens hypertexte) vers d'autres sites syndicaux sur l'intranet ou l'internet (ces renvois seront décidés en cohérence avec l'accès à l'intranet et à l'internet offert aux agents du département ministériel ou du service considéré). ces espaces ont vocation à permettre la mise à la disposition de tout agent raccordé à l'intranet d'informations syndicales.

La mise en ligne des informations sur ces sites intranet sera effectuée par les syndicats, sous leur responsabilité éditoriale et technique. Si ces derniers ne possèdent pas de personne-ressource connaissant les techniques de mise en ligne, l'administration pourra prendre en charge la formation d'adhérents.

#### ***Commentaires du texte concernant la formation***

*Ces possibilités de formation de "spécialistes de la mise à jour de sites" est prévue et vient s'ajouter aux moyens de formation prévus à l'article 1-2.*

### **4. LES FORUMS DE DISCUSSION**

Il sera ouvert la possibilité de forums de discussion, modérés par les organisations syndicales, au sein des sites dont elles disposent sur l'intranet, sous leur responsabilité éditoriale et technique. Les modalités de la modération seront fixées dans les chartes ministérielles.

#### ***Commentaires du texte concernant les forums***

*C'est une autre disposition originale, très favorable aux organisations syndicales, car l'utilisation des forums est interdite dans tous les autres accords d'entreprise.*

## Annexe 2 - 3

### ***Accord " Espaces syndicats "*** ***sur la mise en place d'un panneau d'affichage syndical sur*** ***l'intranet de FRANCE TELECOM*** ***(30 juillet 2000)***

Accord conclu entre les soussignés :

La société France Télécom dont le siège est situé 6, place d'Alleray -75505 PARIS CEDEX 15 - représentée par Bernard BRESSON en sa qualité de Directeur des Ressources Humaines, d'une part,

Et le représentant, dûment mandaté à cet effet", d'autre part. Les parties signataires conviennent des dispositions ci-après :

#### ***Commentaires sur les signataires***

*France Télécom signe un accord avec chaque organisation syndicale : un document par organisation syndicale et non pas un document unique signé par les organisations syndicales.*

*Volonté de mieux faire apparaître les engagements réciproques.*

*Cet accord n'est pas un modèle, mais il peut servir d'exemple pour les autres entreprises.*

#### **PRÉAMBULE**

France Télécom est aujourd'hui la " Net compagnie ". A ce titre, elle souhaite expérimenter pour ses salariés de nouveaux modes d'information basés sur l'Intranet, notamment dans le domaine social.

France Télécom et l'organisation syndicale signataire conviennent sur les bases du présent accord d'ouvrir à compter du 31 juillet 2000 un tableau d'affichage Intranet.

Une analyse de cette première phase d'expérimentation sera faite avec les organisations syndicales en décembre 2000. Cette analyse devra permettre d'évaluer son intérêt et de préciser, si nécessaire, les règles de fonctionnement pour l'exercice 2001 dans l'hypothèse de la poursuite de l'expérimentation.

L'Entreprise se réserve la possibilité de suspendre l'expérimentation à tous moments.

#### ***Commentaires sur la durée de l'accord***

*La plupart de ces accords sont limités à 1 an pour tenir compte de la nécessaire "phase d'expérimentation".*

#### **Article 1 : Principes de base**

L'Entreprise propose à chacun des salariés d'avoir librement accès à l'information syndicale de son choix.

A cet effet, l'organisation syndicale représentative et signataire du présent accord disposera d'un tableau d'affichage électronique sur l'Intranet, sous réserve d'accord aux dispositions ci-dessous.

Celui-ci sera national et distinct des autres organisations. Il n'en sera pas fait de déclinaisons régionales, locales ou en filiales.

### ***Commentaires sur le site unique***

*L'accord ne prévoit pas de sites régionaux contrairement à d'autres accords (ex : Renault)*

France Télécom s'engage, dans le cadre du respect de la liberté individuelle, à ne pas rechercher l'identification des salariés consultant le ou les sites ( art. 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

### ***Commentaires sur le respect des libertés***

Ce rappel est important pour le respect des libertés.

## **Article 2 : Description et situation géographique du matériel**

France Télécom mettra à disposition de l'organisation signataire, dans le local syndical qui lui est affecté par le Secrétaire Général :

- 1 micro-ordinateur
- 1 imprimante
- 1 pack Windows ainsi que le logiciel Front Page.

Le matériel ne pourra en aucun cas être déplacé sauf en cas de modification géographique des locaux souhaités par France Télécom.

Le matériel ci-dessus sera mis gracieusement à disposition de l'organisation signataire par France Télécom. Il ne pourra être utilisé d'autre matériel que celui-ci.

L'hébergement et les frais associés seront à la charge de France Télécom. Les produits consommables (papier, recharges encres. ...) seront à la charge de l'organisation syndicale.

Le matériel sera sous l'entière responsabilité de l'organisation syndicale. Toute disparition de matériel ou détérioration fera l'objet d'un remplacement à l'identique à la charge de l'organisation. L'entretien courant sera assuré par les services informatiques de l'entreprise.

Durant cette phase expérimentale, la capacité de chaque site syndical sera limitée à un maximum de 10 méga octets.

### ***Commentaires sur les moyens***

*Les moyens matériels accordés aux syndicats sont assez importants.*

*Par contre, la place allouée (10 méga octets) semble assez faible quand on sait que tout abonné à Wanadoo dispose de 100 méga octets pour publier un site personnel!*

## **Article 3 : Hébergement des sites**

L'offre Hébergenoo de TRANSPAC est retenue. Cette offre autorise la mise à disposition d'un environnement de pré-production dans lequel l'administrateur du site de l'organisation syndicale effectue les mises à jour du contenu et le visualise avant envoi sur le site de diffusion.

## **Article 4: Accès à l'Intranet France Télécom**

Grâce au matériel mis à disposition, l'organisation syndicale signataire aura également accès au contenu de l'Intranet de l'entreprise à l'exception des services à accès restreint.

Il est rappelé que, s'agissant de communication interne à l'entreprise, les informations contenues dans cet outil ne pourront en aucun cas être utilisées à des usages externes.

Le panneau d'affichage national de l'organisation syndicale sera référencé dans la liste des sites Intranoo sous la dénomination " Espace Syndicats " avec les panneaux des autres organisations hébergées. Au sein du site, il sera identifié par le signe du syndicat.

## **Article 5 : Responsabilité du contenu**

Les communications syndicales affichées sur le panneau d'affichage électronique respecteront les textes légaux en vigueur ainsi que la charte déontologique d'utilisation de l'Intranet du groupe. Il est notamment fait référence au décret 82/447 du 28/05/1982, aux dispositions relatives à la presse mentionnées dans la loi du 29/07/1881 ainsi qu'à l'article L 412/8 du code du travail.

Ces communications seront sous l'entière responsabilité de l'organisation syndicale. En cas d'abus ou de non-respect des textes légaux en vigueur, l'entreprise se réserve la possibilité de porter l'affaire en justice.

### *Commentaires sur la responsabilité éditoriale*

*La responsabilité éditoriale est bien définie : cela est d'autant plus important que la mise à jour du site syndical est faite directement par l'organisation syndicale (article 3)*

## **Article 6 : Utilisation du réseau**

Le tableau d'affichage électronique est conçu pour mettre des informations à destination des salariés du groupe sur un mode conforme à la réglementation des panneaux d'affichage habituels. Ne sont notamment pas autorisées les pratiques suivantes : - le téléchargement de vidéo, d'images animées, de bandes son

- le téléchargement de vidéo, d'images animées, de bandes son
- l'interactivité
- le " streaming " (visualisation de vidéo par le biais du réseau au fur et à mesure du chargement)
- la diffusion de tracts par messagerie
- le spam (diffusion d'un document en grand nombre)
- les forums et le " chat " (causeries interactives) ..
- les " applets " java, moteurs de recherche ou " cookies " (programmes informatiques associés au message)

Toute utilisation abusive, telle que celles mentionnées ci-dessus ou en cas de non-respect de l'accord ou des textes en vigueur quel que soit le mode utilisé (à partir de site Intranet, Internet ou d'un autre site) et quelle que soit l'entité du syndicat concerné (syndicat, fédération, confédération...) entraînera la fermeture immédiate du panneau d'affichage électronique pour une durée d'un mois.

En cas de récidive, il sera définitivement fermé.

### *Commentaires sur les limites d'utilisation*

*L'interactivité (mais le terme n'est pas défini!) est interdite au syndicat! C'est une limite qui fera sourire dans quelques années...*

*Le SPAM est lui aussi interdit, comme dans la plupart des accords ... sauf dans les Recommandations interministérielles sur l'utilisation des TIC par les organisations syndicales dans les fonctions publiques.*

## **Article 7 : Messagerie**

Un lien avec la boîte de messagerie e.mail de l'organisation concernée sera mise en place. Chaque salarié consultant le site aura ainsi la possibilité de laisser un message à l'attention de l'organisation syndicale hébergée sur le site. La réponse ne pourra être qu'individuelle.

Le principe de " chaîne " est interdit et sera sanctionné selon les règles mentionnées à l'article 6.

### *Commentaires sur la messagerie du site syndical*

*Chaque salarié peut laisser un message sur le site syndical : tous les accords d'entreprise ne prévoient pas cette possibilité.*

## **Article 8 : Formation des administrateurs de site**

Pour une utilisation optimale du matériel mis à disposition de l'organisation syndicale, l'entreprise prendra à sa charge la formation de 2 personnes de l'organisation syndicale.

Cette formation devra porter sur :

- les principaux concepts d'Intranet
- les outils de conception et d'édition de pages HTML
- les outils graphiques
- la base du langage HTML

### *Commentaires sur les possibilités de formation*

*chaque salarié de France Télécom étant formé à l'utilisation d'internet, l'accord ne concerne que la formation, plus spécialisée, des administrateurs de site.*

## **Article 9 : Engagement de l'organisation syndicale**

L'organisation syndicale s'engage par sa signature à respecter et à faire respecter dans sa globalité l'accord ci-dessus dès sa date de mise en œuvre.

Fait à Paris le 30 juillet 2000

## Annexe 2 - 4

### *Présentation rapide de quelques exemples d'accords sur l'utilisation des TIC*

#### *2 - 4 - 1 Charte sur l'utilisation des nouvelles technologies de l'information par les syndicats de la Bibliothèque Nationale de France (BNF)*

**Signataires syndicaux:** CFDT et UNSA

**Date de la signature:** 2 octobre 2002

**Objet :** expression syndicale

**Principales dispositions :**

- 1 kiosque électronique syndical est ouvert sur l'intranet
- La messagerie est ouverte à la correspondance individuelle ou à la diffusion limitée.
- Des listes de diffusion peuvent être établies avec l'accord préalable des agents concernés
- Possibilité de lien entre kiosque et messagerie
- Un accord complémentaire sera négocié pour la période des élections

Informations complémentaires : Liaisons sociales du 6 novembre 2002 n° 13761 - page 1

#### *2 - 4 - 2 Accord sur l'accès aux technologies de l'information et de la communication des syndicats et ce de la COGEMA*

**Signataires syndicaux:** 6 syndicats représentatifs (mais entrée en vigueur suspendue à l'adoption d'une charte d'utilisation)

**Date de la signature:** 17 octobre 2002

**Objet :** expression syndicale et CE

**Principales dispositions :**

- Chaque syndicat et CE peut créer un site sur l'intranet (au plus 1 giga octets) respectant la réglementation des panneaux d'affichage
- La messagerie est ouverte à une liste limitée de destinataires identifiés.
- Prise en charge du matériel, des connexions et d'une partie de la formation (2 jours tous les 3 ans)

Informations complémentaires : Liaisons sociales du 6 novembre 2002 n° 13761 - page 1

## Annexe 2 - 5

### *Quelques arrêts de la Cour de cassation*

#### *2 - 5 - 1 Respect de la vie privée dans l'activité professionnelle*

#### **Arrêt de la Cour de cassation du 2 octobre 2001 concernant la confidentialité des fichiers informatiques marqués "personnels"**

On trouvera ci-après les extraits de l'arrêt de la Cour de Cassation - Chambre Sociale du 2 octobre 2001 (voir le texte intégral sur le site du "Forum des droits sur l'internet" (<http://www.foruminternet.org/>) à l'adresse <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=171>)

Il s'agit d'un pourvoi en cassation d'un arrêt rendu le 22 mars 1999 par la Cour d'appel de Paris (procès entre la société Nikon France et un ingénieur salarié M.O.)

Audience publique du 2 octobre 2001  
Cour de Cassation - Chambre Sociale  
M.Waquet, conseiller doyen faisant fonction de président  
Arrêt n°4165 FS-P+B+R+1

Sur le pourvoi incident de M.O.:

Vu l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'article 9 du Code civil, l'article 9 du nouveau Code de procédure civile et l'article L 120-2 du Code du travail,

Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, que celle-ci implique en particulier le secret des correspondances, que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur,

Attendu que pour décider du licenciement d M.O était justifié par une faute grave, la cour d'appel a notamment retenu que le salarié avait entretenu pendant ses heures de travail une activité parallèle, qu'elle s'est fondée pour établir le comportement sur le contenu de messages émis par le salarié, que l'employeur avait découverts en consultant l'ordinateur mis à la disposition de M.O par la société et comportant un fichier intitulé "personnel",

Qu'en statuant ainsi la cour d'appel a violé les textes susvisés;

PAR CES MOTIFS:

CASSE ET ANNULE, dans toutes ses dispositions, l'arrêt rendu le 22 mars 1999...

#### **Rappel des articles cités dans l'arrêt :**

L'arrêt s'appuie sur 4 articles :

- l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

Article 8 de la Convention européenne des droits de l'homme - Droit au respect de la vie privée et familiale

*1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

*2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*

- l'article 9 du nouveau Code civil :

Article 9 du Code civil

*Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.*

- l'article 9 du nouveau Code de procédure civile

Article 9 du nouveau Code de procédure civile

*Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention.*

- l'article L 120-2 du Code du travail :

Article L120-2 du Code du Travail

*Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.*

### **Commentaires sur cet arrêt très important**

1) Cet arrêt rappelle que "le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, ".

*Il rappelle donc qu'il peut exister un espace "vie privée" dans l'espace "vie professionnelle". Cela vient équilibrer le fait que, de plus en plus souvent, un espace "vie professionnelle" vient pénétrer l'espace "vie privée" (travail nomade, téléphone mobile, ...).*

2) Cet arrêt précise qu'un employeur ne peut apporter comme preuve de la faute grave des éléments obtenus en consultant un dossier ou un fichier nommé "personnel" : cela semble induire que si un salarié protège ses fichiers liés à sa vie privée par la mention "Personnel", l'employeur ne peut jamais lire le contenu des fichiers ainsi protégés.

*Mais il faut être conscient des difficultés d'application de ce principe : dans quelle limite le salarié peut-il utiliser les capacités de l'outil mis à sa disposition pour ses besoins personnels?*

*Cela semble aussi induire que, a contrario, un employeur peut lire les autres fichiers non marqués "personnel"*

*Cette disposition va induire un certain nombre de négociations dans les entreprises car devant cette interdiction de consultation, les employeurs vont certainement demander aux salariés respecter un certain nombre de modalités d'utilisation du fichier "personnel":*

- engagement de ne pas mettre de fichiers professionnels dans le dossier "personnel".
- taille maximale du dossier "personnel"
- etc.

*Pour l'utilisation de la messagerie, à notre avis, la meilleure solution serait d'obtenir que chaque salarié dispose d'une double" boîte aux lettres" (voir propositions sur les respect des libertés):*

- *une "boite aux lettres" correspondant à une adresse professionnelle que l'employeur peut ouvrir en cas de nécessité*
- *une "boite aux lettres " correspondant à une adresse "personnelle" que l'employeur ne peut ouvrir*

## 2 - 5 - 2 Représentativité syndicale et Internet

### Arrêt de la Cour de cassation du 2 décembre 2002 concernant la représentativité syndicale et l'utilisation d'internet

Texte intégral sur le site legifrance :

<http://www.legifrance.gouv.fr/WAspad/Visu?cid=110322&indice=1&table=CASS&ligneDeb=1>

La Caisse d'épargne d'Alsace avait attaqué le jugement du tribunal d'instance de Strasbourg qui avait accepté la désignation d'un délégué syndical de la part du syndicat SUD Caisse d'épargne.

La Caisse d'épargne d'Alsace considérait que le syndicat SUD Caisse d'épargne n'était pas représentatif car il ne répondait pas aux deux critères essentiels de représentativité que sont l'ancienneté et l'expérience. Mais le tribunal d'instance de Strasbourg avait reconnu la représentativité du fait de l' "activisme syndical incontestable" déployé par le syndicat SUD Caisse d'épargne.

La Caisse d'épargne estimait :

*"que l'activité déployée suppose l'exercice d'une action syndicale organisée et non d'un simple "activisme syndical" ; qu'en l'espèce, le Syndicat SUD s'était arrogé la possibilité d'utiliser le réseau Internet et les boîtes E-mail des salariés pour diffuser à tout moment des messages syndicaux à l'ensemble du personnel de l'entreprise ; que le juge d'instance estime cependant qu'à la supposer illicite, l'utilisation par Sud du réseau internet et des boîtes E-mail de l'ensemble du personnel, à une fréquence telle qu'elle avait entraîné la saisine du juge des référés par la Caisse d'épargne, révélait à tout le moins "un activisme syndical incontestable" de la part du nouveau syndicat de nature à compenser la défaillance des autres critères ; qu'en statuant ainsi, quand les agissements de ce nouveau syndicat dénotaient au contraire un comportement incompatible avec la reconnaissance de sa représentativité de fait, le tribunal a privé son jugement de base légale au regard des articles L. 133-2 et L. 412-11 du Code du travail."*

Pourtant, la Cour de Cassation a rejeté le pourvoi de la Caisse d'épargne et a donc approuvé le jugement du tribunal d'instance qui reconnaissait la représentativité du syndicat SUD Caisse d'épargne.

#### Commentaires sur cet arrêt

*Cette position de la Cour de cassation est étonnante car l'envoi de messages nombreux aux salariés ("spam syndical") peut être fait par un seul individu et ne peut donc être une marque de représentativité. D'autre part toutes les actions de "spamming" sont très discutables et sont même, maintenant, interdites dans certains cas (directive européenne sur le commerce électronique).*

Informations complémentaires : Commentaires de Jean - Emmanuel Ray, professeur de droit à l'Université de Paris - Sorbonne (Panthéon - Sorbonne) dans le journal "Le Monde" du 7 janvier 2003 (page 20).

## Annexe 2 - 6

### ***Décret du 20 octobre 2005 concernant les correspondants à la protection des données***

*La loi n° 2004-801 du 6 août 2004, loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, a modifié profondément la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

*En particulier, elle a allégé les modalités de déclaration des fichiers à la CNIL en dispensant les entreprises de déclarer leurs fichiers si elles ont désigné un correspondant chargé d'assurer la protection des données.*

*Ce décret du 20 octobre 2005 comporte 8 titres et 100 articles (33 pages !). Cette analyse ne porte que sur le Titre III (articles 42 à 56) qui concerne la possibilité de création d'un correspondant à la protection des données dans chaque entreprise*

*Rappel de la nouvelle rédaction de l'article 22 - III de la loi n° 78-17 du 6 janvier 1978 :*

*" Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.*

*La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés.*

*Elle est portée à la connaissance des instances représentatives du personnel.*

*Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions.*

*Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions.*

*Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. "*

**Décrets, arrêtés, circulaires**  
**Textes généraux**  
**Ministère de la justice**

Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004

*(téléchargeable à l'adresse : <http://www.legifrance.gouv.fr/WAspad/UnDocument?base=LEX&nod=IDE0051309>)*

TITRE Ier : DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS  
TITRE II : DES FORMALITÉS PRÉALABLES À LA MISE EN ŒUVRE DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL  
**TITRE III : DES CORRESPONDANTS À LA PROTECTION DES DONNÉES**  
TITRE IV : DES POUVOIRS DE LA COMMISSION  
TITRE V : DISPOSITIONS PARTICULIÈRES AUX TRAITEMENTS RELEVANT DES ARTICLES 26 ET 42 DE LA LOI DU 6 JANVIER 1978  
TITRE VI : DISPOSITIONS PÉNALES  
TITRE VII : DISPOSITIONS RELATIVES À L'OUTRE-MER  
TITRE VIII : DISPOSITIONS FINALES

**TITRE III**

**DES CORRESPONDANTS À LA PROTECTION DES DONNÉES**

**Chapitre Ier**

Du correspondant à la protection des données à caractère personnel

**Article 42**

La désignation d'un correspondant à la protection des données à caractère personnel par le responsable de traitements relevant des formalités prévues aux articles 22 à 24 de la loi du 6 janvier 1978 susvisée est notifiée à la Commission nationale de l'informatique et des libertés par lettre recommandée avec demande d'avis de réception ou par remise au secrétariat de la commission contre reçu, ou par voie électronique avec accusé de réception qui peut être adressé par la même voie.

*Commentaire :*

*C'est l'entreprise qui désigne ce correspondant à la protection des données (CDP). Si elle notifie son CDP auprès de la CNIL et de l'instance représentative du personnel (voir article 45 ci-après), elle n'a plus à déclarer l'ensemble de ses traitements automatisés et sites web préalablement à leur mise en œuvre.*

**Article 43**

La notification prévue à l'article 42 du présent décret mentionne :

1° Les nom, prénom, profession et coordonnées professionnelles du responsable des traitements, le cas échéant, ceux de son représentant, ainsi que ceux du correspondant à la protection des données à caractère personnel. Pour les personnes morales, la notification mentionne leur forme, leur dénomination, leur siège social ainsi que l'organe qui les représente légalement ;

2° Lorsque le correspondant à la protection des données à caractère personnel est une personne morale, les mêmes renseignements concernant le préposé que la personne morale a désigné pour exercer les missions de correspondant ;

*Commentaires :*

*Le CDP peut être une personne physique ou une personne morale (SSII, ...)*

3° Si la désignation est faite seulement pour certains traitements ou catégories de traitements, l'énumération de ceux-ci ;

4° La nature des liens juridiques entre le correspondant et la personne, l'autorité publique, le service ou l'organisme auprès duquel il est appelé à exercer ses fonctions ;

5° Tout élément relatif aux qualifications ou références professionnelles du correspondant et, le cas échéant, de son préposé en rapport avec cette fonction ;

*Commentaires :*

*Aucune qualification spécifique n'est requise. Mais il paraît évident que le CDP doit avoir une bonne connaissance des techniques informatiques utilisées dans l'entreprise.*

6° Les mesures prises par le responsable des traitements en vue de l'accomplissement par le correspondant de ses missions en matière de protection des données.

L'accord écrit de la personne désignée en qualité de correspondant est annexé à la notification.

La désignation d'un correspondant à la protection des données à caractère personnel prend effet un mois après la date de réception de la notification par la Commission nationale de l'informatique et des libertés.

Toute modification substantielle affectant les informations mentionnées aux 1° à 6° est portée à la connaissance de la Commission nationale de l'informatique et des libertés, dans les formes définies à l'article 42.

#### **Article 44**

Lorsque plus de cinquante personnes sont chargées de la mise en oeuvre ou ont directement accès aux traitements ou catégories de traitements automatisés pour lesquels le responsable entend désigner un correspondant à la protection des données à caractère personnel, seul peut être désigné un correspondant exclusivement attaché au service de la personne, de l'autorité publique ou de l'organisme, ou appartenant au service, qui met en oeuvre ces traitements.

*Commentaires :*

*Cet article induit que les PME de moins de 50 personnes peuvent « mutualiser » un CDP commun à plusieurs PME.*

Par dérogation au premier alinéa :

a) Lorsque le responsable des traitements est une société qui contrôle ou qui est contrôlée au sens de l'article L. 233-3 du code de commerce, le correspondant peut être désigné parmi les personnes au service de la société qui contrôle, ou de l'une des sociétés contrôlées par cette dernière ;

b) Lorsque le responsable des traitements est membre d'un groupement d'intérêt économique au sens du titre V du livre deuxième du code de commerce, le correspondant peut être désigné parmi les personnes au service dudit groupement ;

c) Lorsque le responsable des traitements fait partie d'un organisme professionnel ou d'un organisme regroupant des responsables de traitements d'un même secteur d'activités, il peut désigner un correspondant mandaté à cette fin par cet organisme.

#### **Article 45**

La désignation d'un correspondant à la protection des données à caractère personnel est, préalablement à sa notification à la Commission nationale de l'informatique et des libertés, portée à la connaissance de l'instance représentative du personnel compétente par le responsable des traitements, par lettre recommandée avec demande d'avis de réception.

*Commentaires :*

*Article très important pour le respect des libertés individuelles et collectives : la désignation du CDP doit porter à la connaissance du Comité d'entreprise ou des délégués du personnel.*

#### **Article 46**

Le correspondant à la protection des données à caractère personnel exerce sa mission directement auprès du responsable des traitements.

Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission.

Le responsable des traitements ou son représentant légal ne peut être désigné comme correspondant.

Les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission.

#### **Article 47**

Le responsable des traitements fournit au correspondant tous les éléments lui permettant d'établir et d'actualiser régulièrement une liste des traitements automatisés mis en oeuvre au sein de l'établissement, du service ou de l'organisme au sein duquel il a été désigné et qui, à défaut de désignation d'un correspondant, relèveraient des formalités de déclaration prévues par les articles 22 à 24 de la loi du 6 janvier 1978 susvisée.

*Commentaires :*

*Le CDP doit être informé de tous les traitements et fichiers portant sur des données à caractère personnel.*

#### **Article 48**

Dans les trois mois de sa désignation, le correspondant à la protection des données à caractère personnel dresse la liste mentionnée à l'article 47. La liste précise, pour chacun des traitements automatisés :

- 1° Les nom et adresse du responsable du traitement et, le cas échéant, de son représentant ;
- 2° La ou les finalités de traitement ;
- 3° Le ou les services chargés de le mettre en oeuvre ;
- 4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès et de rectification ainsi que leurs coordonnées ;
- 5° Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- 6° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
- 7° La durée de conservation des données traitées.

La liste est actualisée en cas de modification substantielle des traitements en cause. Elle comporte la date et l'objet de ces mises à jour au cours des trois dernières années.

Le correspondant tient la liste à la disposition de toute personne qui en fait la demande.

Une copie de la liste est délivrée à l'intéressé à sa demande. Le responsable des traitements peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

Lorsque la liste ne recense pas la totalité des traitements mis en oeuvre par le responsable, elle mentionne que d'autres traitements relevant du même responsable figurent sur la liste nationale mise à la disposition du public en application de l'article 31 de la loi du 6 janvier 1978 susvisée.

*Commentaires :*

*Cet article précise que le correspondant tient la liste à la disposition de toute personne qui en fait la demande : cela veut dire, en particulier, que le Comité d'entreprise et les délégués du personnel peuvent disposer de cette liste afin d'événifier qu'aucun traitement n'est « oublié ».*

#### **Article 49**

Le correspondant veille au respect des obligations prévues par la loi du 6 janvier 1978 susvisée pour les traitements au titre desquels il a été désigné.

A cette fin, il peut faire toute recommandation au responsable des traitements.

Il est consulté, préalablement à leur mise en oeuvre, sur l'ensemble des nouveaux traitements appelés à figurer sur la liste prévue par l'article 47.

Il reçoit les demandes et les réclamations des personnes intéressées relatives aux traitements figurant sur la liste prévue par l'article 47. Lorsqu'elles ne relèvent pas de sa responsabilité, il les transmet au responsable des traitements et en avise les intéressés.

Il informe le responsable des traitements des manquements constatés avant toute saisine de la Commission nationale de l'informatique et des libertés.

Il établit un bilan annuel de ses activités qu'il présente au responsable des traitements et qu'il tient à la disposition de la commission.

*Commentaires :*

*Cet article induit que le correspondant à la protection des données doit, en plus de ses compétences informatiques, avoir certaines compétences juridiques.*

#### **Article 50**

Le responsable des traitements peut, avec l'accord du correspondant à la protection des données à caractère personnel, lui confier les missions mentionnées à l'article 49 pour la totalité des traitements qui dépendent du responsable.

Dans ce cas, la notification prévue à l'article 43 en fait mention.

#### **Article 51**

La Commission nationale de l'informatique et des libertés peut être saisie à tout moment par le correspondant à la protection des données à caractère personnel ou le responsable des traitements de toute difficulté rencontrée à l'occasion de l'exercice des missions du correspondant. L'auteur de la saisine doit justifier qu'il en a préalablement informé, selon le cas, le correspondant ou le responsable des traitements.

La Commission nationale de l'informatique et des libertés peut à tout moment solliciter les observations du correspondant à la protection des données ou celles du responsable des traitements.

*Commentaires :*

*Cet article permet au Correspondant à la protection des données, mais aussi au responsable des traitements de faire appel à la CNIL.*

## Article 52

Lorsque la Commission nationale de l'informatique et des libertés constate, après avoir recueilli ses observations, que le correspondant manque aux devoirs de sa mission, elle demande au responsable des traitements de le décharger de ses fonctions en application du III de l'article 22 de la loi du 6 janvier 1978 susvisée.

## Article 53

Hors le cas prévu à l'article 52, lorsqu'il envisage de mettre fin aux fonctions du correspondant pour un motif tenant à un manquement aux devoirs de sa mission, le responsable des traitements saisit la Commission nationale de l'informatique et des libertés pour avis par lettre recommandée avec demande d'avis de réception, comportant toutes précisions relatives aux faits dont il est fait grief.

Le responsable des traitements notifie cette saisine au correspondant dans les mêmes formes en l'informant qu'il peut adresser ses observations à la Commission nationale de l'informatique et des libertés.

La Commission nationale de l'informatique et des libertés fait connaître son avis au responsable des traitements dans un délai d'un mois à compter de la réception de sa saisine. Ce délai peut être renouvelé une fois sur décision motivée de son président.

Aucune décision mettant fin aux fonctions du correspondant ne peut intervenir avant l'expiration du délai prévu à l'alinéa précédent.

*Commentaires :*

*Cet article apporte une certaine protection au correspondant à la protection des données.*

## Article 54

Lorsque le correspondant est démissionnaire ou déchargé de ses fonctions, le responsable des traitements en informe la Commission nationale de l'informatique et des libertés dans les formes prévues à l'article 42.

La notification de cette décision mentionne en outre le motif de la démission ou de la décharge. Il y est annexé, en lieu et place de l'accord prévu au huitième alinéa de l'article 43, le justificatif de la notification de la décision au correspondant.

Cette décision prend effet huit jours après sa date de réception par la Commission nationale de l'informatique et des libertés.

Hormis le cas du remplacement du correspondant, le responsable des traitements est alors tenu de procéder, dans le délai d'un mois, aux formalités prévues aux articles 23 et 24 de la loi du 6 janvier 1978 susvisée pour l'ensemble des traitements qui s'en étaient trouvés dispensés du fait de la désignation à laquelle il est mis fin.

## Article 55

Lorsque le responsable des traitements ne respecte pas ses obligations légales relatives au correspondant, la Commission nationale de l'informatique et des libertés l'enjoint par lettre recommandée avec accusé de réception de procéder aux formalités prévues aux articles 23 et 24 de la loi du 6 janvier 1978 susvisée. Cette lettre mentionne les traitements concernés par l'injonction ainsi que le délai dans lequel le responsable des traitements doit s'y conformer.

## **Chapitre II**

### **Du correspondant à la protection des données appartenant à un organisme de presse écrite ou audiovisuelle**

#### **Article 56**

Le correspondant prévu au quatrième alinéa de l'article 67 de la loi du 6 janvier 1978 susvisée est désigné par le responsable de traitements de données à caractère personnel aux fins de journalisme mis en oeuvre par un organisme de la presse écrite ou audiovisuelle. Ce correspondant est désigné parmi les personnes attachées au service de cet organisme.

Le correspondant est soumis aux dispositions du présent titre, à l'exception des règles relatives à la désignation et aux missions du correspondant prévues par le 2° de l'article 43, l'article 45, les 4° et 7° et les dixième, onzième et douzième alinéas de l'article 48, ainsi que le cinquième alinéa de l'article 49 du présent décret.

## Annexe 3 - 1

### *Convention sur la cybercriminalité adoptée par le Conseil de l'Europe le 8 novembre 2001 à Budapest*

(voir le site du Conseil de l'Europe ( : texte intégral + le rapport explicatif)  
<http://conventions.coe.int/Treaty/FR/cadreprojets.htm>

#### **Présentation**

La Convention a été adoptée par le Comité des Ministres lors de sa 109e Session, le 8 novembre 2001, et est ouverte à la signature, à Budapest, à partir du 23 novembre 2001.

La Convention sera le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques, traitant en particulier des infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux.

Il contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception. Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale".

La Convention est le fruit de quatre années de travail d'experts du Conseil de l'Europe, auxquels étaient associés des experts des États-Unis, du Canada, du Japon et d'autres États non membres de l'Organisation.

Il est prévu de la compléter par un Protocole additionnel visant la criminalisation de toute diffusion de propagande raciste et xénophobe par le biais des réseaux informatiques.

#### *Commentaires du texte de présentation*

*Cette convention doit être ratifiée par les parlements des différents pays signataires, ce qui demandera un délai de plusieurs années. Il faut rappeler que le Conseil de l'Europe regroupe 43 pays membres, c'est à dire beaucoup plus que l'Union européenne.*

*Cette Convention est ouverte à la signature des États membres du Conseil de l'Europe et des États non membres qui ont participé à son élaboration, en particulier les États-Unis, le Canada, et le Japon . Elle entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq États, incluant au moins trois États membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention. (article 36)*

*C'est le premier texte international permettant vraiment la lutte contre la cybercriminalité tout en respectant les droits fondamentaux. (Article 15)*

*Les articles les plus contestés (à tort à notre avis, car il faut prendre les moyens nécessaires à la lutte contre la cybercriminalité) par les défenseurs des libertés sont les articles concernant la perquisition des réseaux informatiques et l'interception :*

*Article 16 – Conservation rapide de données informatiques stockées*

*Article 17 – Conservation et divulgation rapides de données relatives au trafic.*

*Article 19 – Perquisition et saisie de données informatiques stockées*

*Article 20 – Collecte en temps réel des données relatives au trafic*

*Article 21 – Interception de données relatives au contenu*

*Pour le moment, il faut regretter qu'elle ne comporte pas d'article concernant la répression de la propagande raciste et xénophobe.*

*(Les commentaires sur cette convention sont ceux de Yves Lasfargue)*

# Extraits de la Convention sur la cybercriminalité

## [ Conseil de l'Europe - Budapest, 23.XI.2001]

(voir le site du Conseil de l'Europe : texte intégral + le rapport explicatif)

### Préambule

Les États membres du Conseil de l'Europe et les autres États signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres États parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyber-espace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au développement des technologies de l'information ;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace; (...)

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit de ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée; (...)

Sont convenus de ce qui suit:

#### *Commentaires du préambule*

*Ce préambule:*

*- justifie la nécessité d'une coopération internationale pour lutter contre la cybercriminalité*

*- précise que ce texte respecte les garanties individuelles telles que définies dans les différents textes internationaux.(voir article 15).*

## Chapitre I - Terminologie

Article 1 – Définitions

Aux fins de la présente Convention, l'expression:

- a. «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
- b. «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- c. «fournisseur de service» désigne :
- i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;
  - ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;
- d. «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent.

### ***Commentaires de la terminologie***

*On est bien dans un texte concernant les "nouvelles" technologies puisqu'il est nécessaire de définir le vocabulaire!*

*Il faut bien distinguer les données relatives au trafic ( §d) et les données relatives aux contenus, car les contrôles (et les dangers d'atteinte aux libertés) ne seront pas les mêmes.*

## **Chapitre II - Mesures à prendre au niveau national**

### **Section 1 - Droit pénal matériel**

Titre 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 - Accès illégal

Article 3 - Interception illégale

Article 4 - Atteinte à l'intégrité des données.

Article 5 - Atteinte à l'intégrité du système

Article 6 - Abus de dispositifs

Titre 2 - Infractions informatiques

Article 7 - Falsification informatique

Article 8 - Fraude informatique

Titre 3 - Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 - Tentative et complicité

Article 12 – Responsabilité des personnes morales

Article 13 – Sanctions et mesures

## ***Commentaires concernant les mesures à prendre au niveau national en droit pénal***

*Les articles 2 à 13 définissent les différentes infractions. La convention prévoit que chaque état signataire (appelé chaque "partie") doit adopter une réglementation nationale permettant de lutter contre ces infractions.*

### Section 2 – Droit procédural

#### Titre 1 – Dispositions communes

##### Article 14 – Portée d’application des mesures du droit de procédure

##### Article 15 – Conditions et sauvegardes

1. Chaque Partie veille à ce que l’instauration, la mise en oeuvre et l’application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l’homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des droits de l’homme et des libertés fondamentales du Conseil de l’Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966) ou d’autres instruments internationaux applicables concernant les droits de l’homme, et qui doit intégrer le principe de la proportionnalité.

2. Lorsque cela est approprié eu égard à la nature du pouvoir ou de la procédure concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d’autres formes de supervision indépendante, des motifs justifiant l’application ainsi que la limitation du champ d’application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l’intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l’effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.

## ***Commentaires concernant la protection des libertés individuelles et collectives***

*Tout l’équilibre de cette Convention repose sur le respect des ces articles qui rappellent les textes de base, la nécessité de supervision judiciaire et le principe de proportionnalité.*

### Titre 2 – Conservation rapide de données informatiques stockées

#### Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d’ordonner ou d’imposer d’une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d’un système informatique, notamment lorsqu’il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu’une Partie fait application du paragraphe 1 ci-dessus, au moyen d’une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l’intégrité desdites données pendant une durée aussi longue que nécessaire, jusqu’à maximum 90 jours, afin de permettre aux autorités compétentes d’obtenir leur divulgation. Une Partie peut prévoir qu’une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en oeuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation rapides de données relatives au trafic.

1. Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication;

et b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

#### ***Commentaires concernant la conservation rapide des données***

*L'article 16 (§2) prévoit que chaque Partie (c'est à dire chaque pays signataire de la Convention) adopte les mesures législatives pour rendre obligatoire le stockage des données sur une durée pouvant atteindre 3 mois. Évidemment cette obligation ne peut être imposée que par "l'autorité compétente", c'est à dire la justice dans un pays comme la France.*

*Cette possibilité n'est pas scandaleuse, si elle bien placée sous l'autorité de la justice.: il faut se rappeler que c'est un tel stockage de données (concernant les conversations téléphoniques) qui a permis l'arrestation des assassins du préfet de Corse, M.Erignac en 1999.*

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services;

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

#### ***Commentaires concernant l'injonction de produire***

*L'article 18 (§ 1 - b) prévoit que le fournisseur de services peut être obligé, par l'autorité compétente, à communiquer les données en sa possession*

*Cette possibilité n'est pas scandaleuse, si elle bien placée sous l'autorité de la justice.*

#### Titre 4 – Perquisition et saisie de données informatiques stockées

##### Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ;

et b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

##### ***Commentaires concernant la perquisition***

*Cet article 19 prévoit la perquisition et la saisie de données informatiques y compris à distance ( "... ou à accéder de façon similaire" dit le texte).*

*Cette possibilité n'est pas scandaleuse, si elle bien placée sous l'autorité de la justice. La perquisition existe dans le domaine réel et concret (appartement, véhicule, fouilles à corps...) et elle peut aussi exister dans le domaine des informations.*

*Il faut remarquer que ces saisies de données sont parfois réalisées par de nombreux acteurs privés (le plus souvent à l'insu du citoyen et du consommateur) : pour des raisons commerciales par des entreprises privées diverses, pour des raisons d'espionnage industriel par des réseaux d'écoute internationaux (exemple : réseau Échelon des USA et du Royaume Uni) ou pour des raisons de mégalomanie par les "hackers".*

#### Titre 5 – Collecte en temps réel de données informatiques

##### Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire,

ou ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique. (...)

##### ***Commentaires concernant la collecte des données relatives au trafic***

*Cet article 20 prévoit la "collecte en temps réel" des données relatives au trafic.*

*Cette possibilité n'est pas scandaleuse, si elle bien placée sous l'autorité de la justice.*

*Il faut remarquer que ces collectes de données sont parfois réalisées par de nombreux acteurs privés (le plus souvent à l'insu du citoyen et du consommateur) : pour des raisons commerciales par des entreprises privées diverses, pour des raisons d'espionnage industriel par des réseaux d'écoute internationaux (exemple : réseau Échelon des USA et du Royaume Uni) ou pour des raisons de mégalomanie par les "hackers".*

#### Article 21 – Interception de données relatives au contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à :

a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ;

et b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ,

ou ii. Prêter aux autorités compétentes son concours et son assistance

pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique. (...)

#### ***Commentaires concernant la collecte des données relatives au contenu***

*Cet article 21 prévoit la "collecte en temps réel" des contenus, similaire aux "écoutes téléphoniques".*

*Il faut remarquer que ces collectes de contenus sont parfois réalisées par de nombreux acteurs privés (le plus souvent à l'insu du citoyen et du consommateur) : pour des raisons commerciales par des entreprises privées diverses, pour des raisons d'espionnage industriel par des réseaux d'écoute internationaux (exemple : réseau Échelon des USA et du Royaume Uni) ou pour des raisons de mégalomanie par les "hackers".*

#### Section 3 – Compétence

#### Article 22 – Compétence

#### Chapitre III – Coopération internationale

#### Section 1 – Principes généraux

#### Titre 1 – Principes généraux relatifs à la coopération internationale

#### Article 23 – Principes généraux relatifs à la coopération internationale

#### Titre 2 – Principes relatifs à l'extradition

#### Article 24 – Extradition

#### Titre 3 – Principes généraux relatifs à l'entraide

#### Article 25 – Principes généraux relatifs à l'entraide

#### Article 26 – Information spontanée

#### Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

#### Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

#### Article 28 – Confidentialité et restriction d'utilisation

#### Section 2 – Dispositions spécifiques

#### Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

Article 30 – Divulgence rapide de données conservées

Titre 2 – Entraide concernant les pouvoirs d’investigation

Article 31 – Entraide concernant l’accès aux données stockées

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu’elles sont accessibles au public

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

Article 34 – Entraide en matière d’interception de données relatives au contenu

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1. La présente Convention est ouverte à la signature des États membres du Conseil de l’Europe et des États non membres qui ont participé à son élaboration.

2. La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d’acceptation ou d’approbation sont déposés auprès du Secrétaire Général du Conseil de l’Europe.

3. La présente Convention entrera en vigueur le premier jour du mois qui suit l’expiration d’une période de trois mois après la date à laquelle cinq États, incluant au moins trois États membres du Conseil de l’Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4. Pour tout État signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l’expiration d’une période de trois mois après la date de l’expression de son consentement à être lié par la Convention conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

Article 38 – Application territoriale

Article 39 – Effets de la Convention

Article 40 – Déclarations

Article 41 – Clause fédérale

Article 42 – Réserves

Article 43 – Statut et retrait des réserves

Article 44 – Amendements

Article 45 – Règlement des différends

Article 46 – Concertation des Parties

Article 47 – Dénonciation

Article 48 – Notification

### ***Commentaires concernant l’entrée en vigueur***

*Cette Convention est soumise à ratification, acceptation ou approbation par chacune des Parties (c’est à dire les 43 membres du Conseil de l’Europe, et divers autres pays dont les USA, le Canada et le Japon).*

*Elle entrera en vigueur le premier jour du mois qui suit l’expiration d’une période de trois mois après la date à laquelle cinq États, incluant au moins trois États membres du Conseil de l’Europe, auront exprimé leur consentement à être liés par la Convention.*

*Ces délais risquent de donner du temps aux cybercriminels!*

## Annexe 4 - 1

### ***12 propositions de la CFDT Cadres sur l'utilisation des technologies de l'information et de la communication dans les entreprises et les administrations<sup>11</sup>***

(voir le site de la CFDT Cadres <http://www.cadres-plus.net/>)

#### ***La consultation des instances représentatives du personnel (IRP) sur les Intranets DRH***

##### **Proposition 1 : Consultation des IRP sur les Intranets DRH**

Tout projet d'Intranet DRH (système Intranet permettant à la Direction des Ressources Humaines de diffuser un certain nombre d'informations aux salariés doit faire l'objet d'une consultation des instances représentatives du personnel conformément à l'article L432-2 du Code du travail.

#### ***La négociation de chartes Intranet dans les entreprises et administrations***

##### **Proposition 2 : Négociation avec les organisations syndicales et consultation des IRP**

Toute mise en place de charte d'utilisation des TIC doit faire l'objet d'une négociation collective préalable avec les organisations syndicales. Afin de lui donner force juridique, la charte est intégrée ou annexée au règlement intérieur. Le Comité d'entreprise doit être préalablement consulté, conformément à l'article L122-36 du code du travail. Dans les administrations, le Comité technique paritaire compétent est préalablement consulté.

##### **Proposition 3 : Articulation charte Intranet / Règlement intérieur / Contrat de travail**

L'entreprise ne peut exiger de chaque salarié une signature individuelle de la charte Intranet, document collectif, modifiant le règlement intérieur s'applique à l'ensemble des salariés. Si toutefois les règles négociées induisent une modification spécifique du contrat de travail, celle-ci doit donner lieu à négociation avec le salarié.

#### ***La négociation d'un accord " Intranet syndical "***

##### **Proposition 4 : Utilisation de l'Intranet par les organisations syndicales et par les instances représentatives du personnel**

Dans toute entreprise ou administration utilisant un réseau Intranet, un accord doit être négocié pour déterminer les règles d'utilisation de l'Intranet par les organisations syndicales et les instances représentatives du personnel.

##### **Proposition 5 : Possibilité de listes de diffusions syndicales**

Dans toute entreprise ou administration utilisant un réseau Intranet, il doit être possible de mettre en place une " liste de diffusion " sur le site Intranet syndical, permettant une diffusion nominative de messages.

##### **Proposition 6 : Possibilité de diffusion à tous les salariés**

En période d'élections, une possibilité d'envoi de messages syndicaux à tous les salarié(s) doit être prévue. Cette possibilité d'envoi existe déjà, sous forme de documents papier par la poste, dans les élections politiques ou prud'homales (présentation de chaque candidature envoyée à tous les électeurs).

---

<sup>11</sup> Ces propositions ont été complétées par « 15 propositions sur le télétravail » de décembre 2004 (voir la brochure « Négocier le télétravail » téléchargeable sur le site [www.ergostressie.com](http://www.ergostressie.com))

### **Proposition 7 : Moyens financiers et techniques pour faire fonctionner l'Intranet syndical**

Tout accord concernant l'utilisation de l'Intranet par les organisations syndicales doit prévoir les moyens matériels, financiers et de formation permettant à l'organisation syndicale de maîtriser et de faire fonctionner l'Intranet syndical.

Sur le plan technique, afin d'assurer un certain équilibre dans la diffusion des informations, le site syndical Intranet doit profiter des mêmes possibilités de diffusion que celles offertes par l'Intranet DRH ou celles offertes classiquement à un internaute sur internet : interactivité, utilisation du multimédia, utilisation des " cookies ", utilisation de la fonction téléchargement, possibilité de forum modéré, accès à d'autres sites internes ou externes par liens.

### **Proposition 8 : Respect des libertés individuelles et confidentialité des messages syndicaux**

La confidentialité des contenus des messages, mais aussi des destinataires et émetteurs de messages (qui écrit à qui? Quand? Combien de fois?) et la confidentialité des appels sur le site syndical (qui appelle? Quand? Combien de fois?) doit être garantie par l'entreprise ou l'administration. Cela est vrai pour les messages syndicaux comme pour tous les autres messages personnels.

## ***La négociation des règles garantissant le respect des libertés individuelles***

### **Proposition 9 : Respect des libertés individuelles et double " boîte à lettres "**

La confidentialité des messages " personnels " doit être garantie par l'entreprise, comme l'a confirmée l'arrêt de la cour de cassation du 2 octobre 2001. La mise en place d'une boîte à lettre personnelle (exemple: persomartin@entreprise.fr), à côté de la boîte à lettre professionnelle (exemple : martin@entreprise.fr), sur le même Intranet d'entreprise, offre une solution pertinente pour répondre aux besoins de confidentialité des messages, de respect de la vie privée dans l'activité professionnelle.

### **Proposition 10 : habilitation des administrateurs de réseaux et le "droit de discrétion"**

La gestion technique des réseaux et des fichiers, et en particulier la gestion de la sécurité, exige parfois que les administrateurs de réseaux puissent prendre connaissance des contenus de messages ou de fichiers concernés par les lois de protection des données individuelles, comme l'a remarqué l'arrêt de la Cour d'appel de Paris du 17 décembre 2001.

Cette prise de connaissances ne doit se faire que dans la mesure où :

- a) Elle n'est pas faite à l'insu des salariés concernés par ces informations
- b) Elle est reconnue comme étant nécessaire au bon fonctionnement du réseau. Cette reconnaissance est concrétisée par une "habilitation à "prendre connaissance des contenus" qui doit être marquée explicitement dans le contrat de l'administrateur de réseaux et accompagnée d'un engagement de confidentialité de la part de l'administrateur de réseau.
- c) Elle est accompagnée de l'engagement de l'entreprise à faire respecter le "droit de discrétion", c'est à dire à ne pas demander à l'administrateur de réseaux de révéler les contenus dont il aura pris connaissance.
- d) Elle fait l'objet d'une négociation avec les organisations syndicales sur les modalités d'utilisation.
- e) La personne habilitée ne peut pas être le chef d'entreprise ou un membre de sa famille.

**Proposition 11 : habilitation de certains salariés à prendre connaissance des données individuelles des fichiers de gestion des Ressources humaines.(fichiers administratifs, e-learning,...)**

Les systèmes d'ERM (Employee Relationship Management ou GRS - Gestion de la Relation avec les Salariés) ont pour objectif de regrouper des informations individuelles sur chaque salarié, informations autrefois dispersées sur des supports divers.

Toute mise en place, explicite ou implicite de tels systèmes doit s'accompagner :

- a) d'une déclaration à la CNIL des nouveaux fichiers ainsi constitués, physiquement ou logiquement.
- b) d'une définition très précise des utilisations possibles et des personnes habilitées à consulter ces informations. Par exemple: qui peut consulter les résultats des exercices effectués en e-learning? L'habilitation à "prendre connaissance de certaines informations individuelles concernant les salariés" doit être explicite dans le contrat du salarié habilité et accompagnée d'un engagement de confidentialité de la part de ce salarié.
- c) d'une négociation avec les organisations syndicales sur les modalités de fonctionnement de ces habilitations.
- d) d'une consultation du Comité d'Entreprise dans le cadre de l'article L 432 - 2 du Code du travail.

***Le droit à la déconnexion pour les salariés***

**Proposition 12 : Droit à la déconnexion**

Les frontières entre vie privée et vie professionnelle deviennent de plus en plus floues, plus particulièrement pour les cadres et les travailleurs nomades. Des négociations doivent s'engager avec les organisations syndicales, dans les entreprises et les administrations, pour prendre en compte ces nouvelles réalités professionnelles et faire reconnaître pour chaque salarié un véritable droit à la déconnexion, en particulier pour éviter les astreintes insidieuses.

## ***Les publications de l'OBERGO***

*(4 documents mis à jour et téléchargeables gratuitement sur [www.ergostressie.com](http://www.ergostressie.com))*

**Yves Lasfargue**

### ***EVOLUTIONS DU TRAVAIL dans la société de l'information***

***Présentation  
de l'ergostressie***

***Brochure n°1:***

*Présentation des évolutions du travail  
et des principes de la mesure de la  
charge de travail par le niveau  
d'ergostressie*

**Yves Lasfargue**

### ***KIT DE MESURE DE LA QUALITE DE VIE AU TRAVAIL***

***Brochure n°2:***

*10 tests d'auto évaluation de ses  
conditions de travail et de mesure de  
son niveau d'ergostressie*

**Yves Lasfargue**

### ***INTERNET, DROITS DES SALARIE(E)S et intranets syndicaux***

**Yves Lasfargue**

### ***NEGOCIER LE TELETRAVAIL***

***Exemples  
d'accords  
et de contrats***

# Obergo

Observatoire des conditions de travail et de l'ERGOstressie

**L'OBERGO** (OBServatoire des conditions de travail et de l'ERGOstressie) est une cellule de recherche créée par Yves Lasfargue pour mettre au point et diffuser des outils de réflexion et de formation sur les conditions de travail et les relations sociales.

OBERGO - 7, rue de l'arbre aux 40 écus 92 390 Villeneuve la Garenne FRANCE

Téléphone : + (33) (0)6 81 01 98 72

Courriel : yves.lasfargue@wanadoo.fr

Site Internet sur les conditions de travail dans la société de l'information: [www.ergostressie.com](http://www.ergostressie.com)

Numéro URSSAF : 920 781827131001003

Numéro SIRET : 430 468 637 00011

Code APE : 722A

Sur le site [www.ergostressie.com](http://www.ergostressie.com), on trouve la présentation de l'OBERGO (OBServatoire des conditions de travail et de l'ERGOstressie) et en accès libre totalement gratuit les rubriques suivantes :

- \* **MESURER** sa charge de travail, son ergostressie, son temps de travail "complet" et l'équilibre de ses temps à l'aide du « Kit de mesure de la qualité de vie au travail dans la société de l'information » et de la suite logicielle LUCIDITY 1, 2, 3 © (systèmes experts permettant l'analyse des conditions de travail),
- \* **NEGOCIER** le télétravail (accord collectif et contrat individuel), les intranets syndicaux et les tracts électroniques
- \* **FAIRE RESPECTER** les libertés et les droits des salariés concernant l'usage d'Internet et des intranets
- \* **AGIR** pour éviter les exclusions et pour éviter l'explosion de la bulle sociale Internet
- \* **CONSULTER** les publications et les conférences d'Yves Lasfargue et une bibliographie sur le travail



L'ensemble de cette création logicielle est mis à disposition sous un [contrat Creative Commons](http://creativecommons.org/)  
(voir tous les détails sur le site : <http://creativecommons.org/>)

*Conçue par Yves Lasfargue et réalisée par Philippe Médan, la suite logicielle LUCIDITY 1, 2, 3 © peut être adaptée sur demande aux spécificités de toute entreprise ou de toute institution (vocabulaire spécifique, règles particulières, commentaires,...) et peut être INSTALLÉE SUR L'INTRANET DE VOTRE ENTREPRISE.*

**[www.ergostressie.com](http://www.ergostressie.com)**

***Pour être LUCIDE et AGIR sur les conditions de travail***