



# La protection des données à caractère personnel dans l'entreprise

Etienne Wéry

Avocat aux barreaux de Bruxelles et Paris

Associé ULYS

[www.uly.net](http://www.uly.net)

## Plan

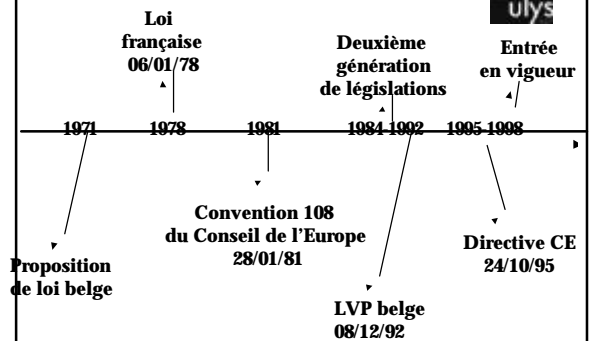


1. Historique belge, européen et international
2. Principes de base de la LVP
3. Principe de finalité, de conformité des données et de licéité du traitement
4. Protection accrue de certaines données
5. Les droits des personnes concernées
6. Les obligations du responsable du traitement
7. Répression et responsabilité
8. Vie privée et communications électroniques
9. La protection de la vie privée des travailleurs
10. Nouvelles technologies problématiques du point de vue de la vie privée

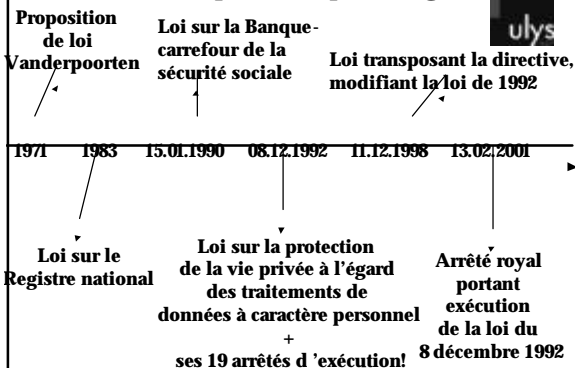


## Première partie : Historique belge, européen et international

### 1. Historique sur le plan international



### 2. Historique sur le plan belge



## Historique sur le plan belge



- La Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981)
- La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel  
.... et ses 19 arrêtés d'application
- La directive européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

## Historique sur le plan belge

- La loi du 11 décembre 1998 transposant la directive et l'arrêté royal du 13 février 2001
- Directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.-> article 14 de la loi du 11 mars 2003.
- Convention collective n°81 relative à la protection de la vie privée des employeurs à l'égard du contrôle des données de communication électroniques en réseau

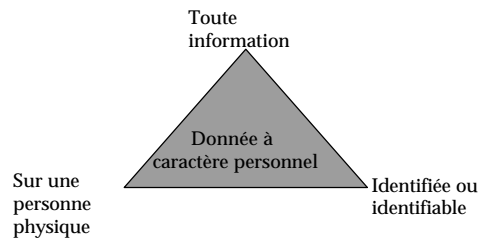
## Deuxième partie : Principes de base de la loi

### 1. Principe de base de la LVP

#### Équilibre entre :

- Le droit des « fumeurs » de traiter les données personnelles
- Le droit des « fichés » de contrôler ce traitement

### 2. Notions de base



### « toute information »

- Exemples :
  - Information écrite ou chiffrée
  - Information contenue dans une image, une bande son
  - Une empreinte digitale
  - Toute information, peu importe la forme

### « une personne identifiée »

- Informations relatives à une personne identifiée
- Donc la loi ne s'applique pas aux personnes morales (sauf Italie, Luxembourg, Autriche et Suisse!)
- La loi s'applique néanmoins aux fichiers B to B s'ils contiennent des informations sur des personnes physiques (personnel, administrateurs, directeurs etc.)

## « Personne physique identifiable »

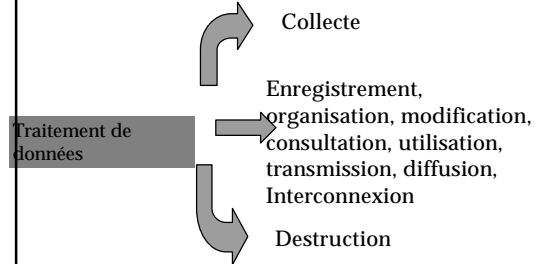


Art. 1er, § 1er de la loi: « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »

Exposé des motifs: « prendre en compte l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement ou par toute autre personne, pour identifier les sujets des données. »

In abstracto

## Notion de « traitement de données »



## Traitements



### • **Automatisés** : 2 conditions :

- Existence d'une ou plusieurs opérations effectuées sur les données
- Utilisation de procédés automatisés

### • **Non automatisés** : 3 conditions

- Existence d'une ou plusieurs opérations effectuées sur les données
- Existence d'un fichier
- Utilisation de procédés non automatisés

**Opérations** : une seule opération suffit : collecte d'info, conservation de données, visionnage d'images sur Internet, consultation d'une base de donnée...

**Procédés automatisés** : englobe n'importe quel procédé « intelligent » qui permet d'effectuer des opérations sur les données

**Procédés non automatisés** : toute technique qui ne nécessite pas l'utilisation d'une machine.

**Fichier** : données accessibles selon un critère / structuration qui facilite l'accès et l'utilisation des données (pas des fichiers eux-mêmes)

## Notion de « responsable du traitement »



- Critère : celui qui détermine les finalités et moyens.
- Personne physique ou morale, association de fait ou administration.
- Il peut y avoir plusieurs responsables si détermination conjointe des finalités et moyens.

• **Difficulté pratique** : Qui détermine les finalités et moyens au sein d'un groupe d'entreprises (une entité juridique décide pour les autres ou décision provenant de plusieurs entités)?

## Notion de « sous-traitant »



- C'est celui qui traite les données pour le compte du responsable
- Doit être de « qualité »

### • **Par exemple** :

- Le prestataire informatique
- Le secrétariat social
- Le gestionnaire marketing des clients

### 3. Champ d'application de la loi

#### Exclusions

totale

Traitements liés à des activités exclusivement personnelles ou domestiques

partielles

Traitements effectués à des fins de sécurité publique

Traitements effectués à des fins de journalisme ou d'expression littéraire et artistique

### 4. Champ d'application territorial

- Critère d'application de la LVP : lieu de l'établissement fixe du responsable



À savoir, le lieu d'exercice effectif et réel d'une activité au moyen d'une installation stable

- Si pas d'établissement sur le territoire de la CE : LVP s'applique dès qu'il y a un recours à des moyens situés sur le territoire belge, dans le but de traiter des données personnelles, sauf le simple transit de données sur le territoire

### Troisième partie :

Principes de finalité et de licéité du traitement ; Principe de conformité des données

### 1. Principe de finalité



#### Principe de légitimité:

-Finalité déterminée (précise) et explicite (pas secrète)

-Finalité légitime : Le but ne peut induire une atteinte disproportionnée aux intérêts des personnes

#### Principe de conformité :

-Utilisation des données en conformité avec la finalité légitime déclarée

-Données adéquates, pertinentes et non excessives par rapport à la finalité déclarée

### Une finalité légitime 6 hypothèses

1) Consentement indubitable de la personne concernée

- Libre
- Éclairé
- Spécifique
- forme libre

2) Nécessaire au contrat ou à la négociation d'un contrat

### Une finalité légitime 6 hypothèses

3) Nécessaire au respect d'obligations légales (ex : congés de maternité, etc.)

4) Nécessaire sauvegarde de l'intérêt vital (ex : santé)

5) Mission d'intérêt public/autorité publique (ex : police)

6) Intérêt légitime du responsable du traitement pour autant que ne prévalent pas l'intérêt ou les droits et libertés de la personne concernée

## Une finalité légitime



- 6ème hypothèse suppose 3 éléments:
  - Existence d'un intérêt légitime (càd non contraire à une loi)
  - Lien de nécessité entre l'existence du traitement et la réalisation de l'intérêt légitime : choix de la voie la moins dommageable du point de vue du respect de la vie privée
  - Prédominance de l'intérêt légitime

## Compatibilité des finalités



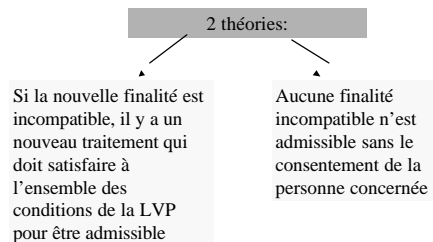
- Une fois annoncée, la finalité doit être respectée
- Les données ne peuvent être utilisées de manière incompatible avec la finalité annoncée
- On tient compte des prévisions raisonnables des intéressés et des dispositions légales

## Exemples d'incompatibilité



- Utilisation à des fins commerciales des données collectées en vue de la réalisation d'un annuaire téléphonique
- Utilisation des photos d'un badge d'identification pour la réalisation d'une brochure de présentation de l'entreprise
- Utilisation du fichier clientèle à des fins de prospection marketing tout à fait différente

## Quid en cas d'incompatibilité?



## 2. Principe de conformité



- Données adéquates, pertinentes et non excessives par rapport au but recherché
- Il faut examiner au cas par cas quelles données sont vraiment nécessaires pour réaliser l'objectif poursuivi.
- Durée de conservation des données limitée.
- La durée de conservation ne peut excéder celle nécessaire à la réalisation de la finalité.

## 3. Licéité du traitement de données



Données traitées loyalement

Traitées en toute transparence : information de la personne concernée

Données traitées licitement

Traitement respectueux des lois : LVP, loi e-commerce pour l'envoi de courriels à des fins de marketing, ...



## Quatrième partie : Protection accrue de certaines données

## 1. Catégories particulières de données



- **Données « sensibles »** : révèlent l'origine raciale ou ethnique, les opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données relatives à vie sexuelle.
- **Données relatives à la santé**
- **Données judiciaires** : relatives à des suspicions, poursuites, condamnations pénales ou administratives

## 2. Données sensibles et médicales



- **Principe : interdiction de traiter les données**  
sauf si

- consentement par écrit (Non autorisé pour les employeurs!)
- données manifestement publiques
- associations à finalité politique, religieuse,... et pas de communication à des tiers
- obligation légale (droit du travail)
- permis par ou en vertu d'une loi, en vue de l'application de la sécurité sociale ou pour un motif d'intérêt public important ...

- aux fins de médecine préventive, de diagnostic médicaux, de l'administration de soins, et le traitement est effectué sous la surveillance d'un professionnel des soins de santé

## 3. Données judiciaires



- **Principe: interdiction de traiter les données**

Sauf :

- sous contrôle autorité publique
- si nécessaire exécution loi ou obligations réglementaires
- gestion contentieux
- avocats

## 4. Précautions particulières



- désigner les catégories et fonctions des personnes ayant accès aux données
- lors de l'information, mentionner la base légale autorisant le traitement de données sensibles
- si consentement écrit, signaler les motifs du traitement de données sensibles et catégories de personnes ayant accès aux données

## Cinquième partie: Les droits des personnes concernées



## 1. Droit d'être informé



### De quoi?

- Au moins : identité resp. du traitement, finalités, droit de s'opposer au traitement à fins de « direct marketing »
- Information supplémentaire : existence droit d'accès et rectification, destinataires des données, caractère obligatoire ou facultatif de la réponse (suite à un demande d'accès) et conséquences du défaut de réponse

## Droit d'être informé



- Quand?
  - Lors de la collecte, si informations collectées auprès de la personne concernée
  - Lors de l'enregistrement ou de la communication
- Exception:
  - Impossible ou efforts disproportionnés : il faut justifier et indiquer les motifs dans la déclaration
  - Il faudra informer dès le premier contact avec la personne concernée

## Droit d'être informé



### Exemples :

- Insertion d'une clause type dans un questionnaire, courrier, sur un site web
- Dans une relation contractuelle : insertion de l'information dans le contrat ou dans les conditions générales
- Information orale par téléphone
- Note interne aux employés de l'entreprise

## 2. Droit d'accès



- Quoi ?
  - Confirmation que des données sont ou non traitées
  - Données contenues à son sujet
  - Origine
  - Connaissance de la logique du traitement
  - Information sur le droit d'exercice des recours relatifs à la rectification (Tribunal de 1ère instance)
- Exceptions :
  - Journalisme, expression littéraire ou artistique si compromettrait publication

## Droit d'accès



- Forme :
  - Courrier du demandeur daté et signé avec une photocopie de la carte d'identité
  - Par courrier postal, par e-mail ou tout autre voie de communication



Le responsable du traitement à l'obligation de contrôler l'identité du demandeur!

## Droit d'accès



- Réponse du responsable du traitement
  - Délai de réponse de maximum 45 jours
  - Mais le responsable du traitement a néanmoins l'obligation de tout mettre en oeuvre pour répondre au plus vite
  - Vérification de la recevabilité (pas obligation de répondre à de multiples demandes dans un même délai)
  - Pas de forme particulière

## Droit d'accès indirect



- **Données relatives à la santé :**
  - Choix du patient: accès direct OU par l'intermédiaire d'un professionnel
  - Possibilité pour le responsable d'exiger un intermédiaire choisi par le patient
- **Données traitées par la « police » :**  
Accès via la Commission de la protection de la vie privée

## 3. Droit de rectification :



- rectification de toute donnée inexacte,
- ou suppression
- et interdiction d'utilisation de donnée incomplète, non pertinente ou conservée pour une durée trop longue par rapport à la finalité poursuivie.



- **En pratique:**
  - Le demandeur doit apporter une preuve de l'inexactitude des données...
  - La demande doit porter sur des données objectives (nom, adresse, etc)
  - Le responsable doit indiquer l'existence d'une contestation en cas de communication des données à des tiers

## 4. Droit d'opposition



- Sur demande datée et signée, droit de s'opposer :
  - Pour raisons sérieuses et légitimes
  - Sans justification en cas de traitements à fins « direct marketing »

## Refus des décisions individuelles automatisées



- Ne pas être soumis à décision produisant **effets juridiques** à l'égard d'une personne ou l'affectant de manière significative, prise sur seule fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité
- **Exceptions :** contrat ou disposition légale si garantie de sauvegarde des intérêts de la personne et de son point de vue.

## Sixième partie : Les obligations du responsable du traitement



## 1. Déclaration du traitement



- Auprès de la Commission de la protection de la vie privée : [www.privacy.fgov.be](http://www.privacy.fgov.be)
- Obligatoire pour les traitements automatisés
- Ce n'est pas une procédure d'autorisation : c'est une obligation purement administrative de déclaration
- Accusé de réception dans les trois jours

PARTIE I. Responsable du traitement

Nom et prénom du responsable du traitement

HM

1. Le responsable de traitement (relève par obligation)

N° de déclaration de la personne physique de l'association de loi 114 et de l'administration publique

Titulaire du traitement de données à caractère personnel (cf. art. 1)

Adresse postale du responsable

Titulaire du traitement de données à caractère personnel

SI existe, le numéro d'INSEE

SI existe, le numéro de TVA

Rue

Cod postal  Commune

Déclaration-type sur le site [www.privacy.fgov.be](http://www.privacy.fgov.be)

## Exceptions à l'obligation de déclarer intéressants les entreprises



- Administration des salaires des personnes au service du / travaillant pour le responsable du traitement

**Par exemple** : salaires, notes de frais, opérations pour le calcul des rémunérations, des cotisations, données requises dans des documents sociaux, données liées à des obligations découlant du droit du travail, de la sécurité sociale et fiscal – **condition** : utilisation des données dans le cadre de la finalité d'administration des salaires

## Exceptions à l'obligation de déclarer



- Traitements relatifs au personnel :
  - ça couvre toutes les finalités de traitement présentes dans le cadre de la relation de travail, excepté ce qui est relatif à l'administration des salaires
  - Par exemple : finalités liées au recrutement, à la formation ou à l'évaluation du travail
  - L'exception tombe pour les données sensibles, « santé » et judiciaires
  - L'exception tombe aussi pour les données liées à l'évaluation de la personne concernée

## Exceptions à l'obligation de déclarer



- Traitements relatifs à la comptabilité
- Traitements relatifs à l'administration des données d'actionnaires et d'associés
- Traitements relatifs à la gestion de la clientèle et des fournisseurs
- Traitements relatifs à l'enregistrement des visiteurs dans le cadre des contrôles d'accès
- Traitements visant l'identification et la localisation de personnes (traitements visant à entretenir des relations sociales ou professionnelles – par exemple envoi d'invitations, convocation à une réunion)

## 2. Sécurité et confidentialité



- Faire diligence pour tenir les données à jour
- Limiter l'accès du personnel aux seules données nécessaires
- Mettre le personnel au courant des obligations découlant de la législation : le personnel est lié par l'obligation de confidentialité

## Sécurité et confidentialité



- Mesures techniques et organisationnelles requises pour protéger les données
  - En tenant compte de l'état de la technique,
  - des frais
  - et de la nature des données à protéger

Prévention contre le piratage informatique  
Prévention contre les malveillances internes  
-> insertion d'une clause de confidentialité dans le contrat de travail

## Sécurité et confidentialité



- Choix du sous-traitant et garanties contractuelles
  - choix d'un sous-traitant qui offre des garanties suffisantes quant à la sécurité
  - contrat doit fixer responsabilité du sous-traitant et indiquer que le sous-traitant ne peut agir que sur instructions du responsable

## Septième partie : Répression et responsabilité



## 1. Responsabilité du responsable du traitement



### Sanctions civiles

- Acte contraire à la LVP
- dommage
- lien de causalité



Responsable du traitement = responsable

Exonéré si prouve que dommage ne lui est pas imputable (faute de la victime, d'un tiers)

## 2. Sanctions pénales



- De 500 à 500 000 € selon le délit
- En cas de récidive, possibilité de peine d'emprisonnement de 3 mois à 2 ans!
- Peines accessoires : confiscation des supports matériels, effacement des données

## 3. Recours



- Plainte CPVP
- Recours judiciaires

### Compétences de la Commission de la protection de la vie privée

- Compétence d'avis: nature (avis d'initiative ou demande d'un organe légis. ou exéc.), motivés, délai
- Compétence de recommandations
- Compétence d'examen des plaintes et de dénonciation au parquet
- Compétence d'homologation des codes de conduite
- ≠ Compétence juridictionnelle



## Huitième partie : Vie privée et communications électroniques



### Plan

- Cadre normatif
- Champ d'application de la directive 2002/58
- Obligation de sécurité
- Obligation de confidentialité
- Données de trafic
- Les autres données de localisation
- Disposition anti-spamming



### 1. Cadre Normatif

- Directive 2002/58 « vie privée et communications électroniques », qui abroge l'ancienne directive 97/66.
- La directive « cadre » du « package Telecom » : directive 2002/21.



### 2. Champ d'application de la directive 2002/58

- Traitements de données à caractère personnel
- dans le cadre de la fourniture de services de communications électroniques
- accessibles au public sur les réseaux publics de communications dans la Communauté.



### Champ d'application de la directive 2002/58

- S'applique aux réseaux publics, pas aux réseaux privés ou d'entreprise.
- S'applique aux services de transmission de signaux, pas aux services de contenu (>< services de la société de l'information : directive e-commerce).
- Ne concerne pas la radiodiffusion, mais bien les services de vidéo à la demande.
- S'applique aussi aux personnes morales : aux « abonnés » (>< Directive 95/46)



### 3. Obligation de sécurité

- Obligation à charge des fournisseurs de services de communications électroniques
- de prendre les mesures d'ordre technique et organisationnel appropriées pour garantir la sécurité des services

## 4. Obligation de confidentialité



- Les Etats membres doivent garantir:
  - la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public,
  - ainsi que la confidentialité des données relatives au trafic y afférentes.

Interdiction d'écouter, d'intercepter, de stocker les communications et données de trafic, sauf pour l'utilisateur lui-même.

## Obligation de confidentialité



- S'applique aux communications et
- Aux données de trafic y afférentes

Toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation

### • Exceptions :



- si autorisation légale, notamment en matière d'enregistrement destiné à fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.
- le stockage technique nécessaire à l'acheminement d'une communication est permis,
- Utilisation des cookies : OK si l'utilisateur est informé de la présence du cookies, de leur mode de fonctionnement, des finalités et du droit d'opposition.
- stockage ou accès techniques exclusivement destinés à effectuer ou faciliter la transmission d'une communication
- stockage ou accès techniques nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

## 5. Données de trafic



- Les données de trafic stockées doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication
- Traitement plus long : OK pour
  - La facturation et l'établissement des paiements pour interconnexion
  - La commercialisation des services de communications électroniques ou la fourniture de services à valeur ajoutée

➡ Si information de l'abonné ou utilisateur

## 6. Les autres données de localisation



- Peuvent être traitées si
  - rendues anonymes
  - ou moyennant le consentement de l'utilisateur ou abonné
  - pour la durée nécessaire à la fourniture d'un service à valeur ajoutée.

Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation à traiter.

## 7. Disposition anti-spamming



- Principe de l'opt-in : consentement PREALABLE
- Pour les courriers électroniques

« tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère »

• E-mails, sms, mms, etc

## Transposition en droit belge



- Loi du 11 mars 2003 relative à certains aspects juridiques des services de la société de l'information
- AR du 4 avril 2003 visant à réglementer l'envoi de publicités par courrier électronique

## Exception au principe de l'opt-in



Opt-out :

- Lorsque les données ont été obtenues auprès des clients du prestataire, personnes physiques ou morales
- lorsque les données ont été recueillies auprès de personnes morales, pour autant que les coordonnées électroniques utilisées à cette fin soient impersonnelles.

Par exemple : Info@...  
commandes@....

## Neuvième partie : La protection de la vie privée des travailleurs



## Plan



- Cadre normatif
- Application razione personae
- Application razione materiae de la CCT n° 81
  - Principe de finalité
  - Principe de proportionnalité
  - Principe de transparence
  - Procédures d'individualisation

## 1. Cadre normatif



### Le cadre général

- Article 8 Convention européenne des droits de l'homme
- Article 22 Constitution
- Article 109 ter D et E de la loi du 21 mars 1991 (loi Belgacom)
- Article 314 bis du Code pénal
- Loi du 8 décembre 1992 (loi vie privée)

## 1. Cadre normatif



### Un nouvel instrument : la CCT n° 81

Convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau

- CCT interprofessionnelle, rendue obligatoire par AR du 12 juin 2002.
- Question de la validité d'un AR qui déroge à la loi!

## 2. Application ratione personae



- Cadre général = applicable au secteur public
- La CCT n° 81 = applicable, en principe, au secteur privé

- Pour les administrations
  - Dualité du personnel :
    - **Contractuels** => L. 3/07/1978 sur les contrats de travail
    - **Statutaires** => Statut administratif + régime disciplinaire de la loi communale
  - Obligation de disposer d'un règlement de travail (loi du 8 avril 1965, modifiée par la loi du 18 décembre 2002)
  - Possibilité de règlements de travail différents (contractuel/statutaire)
  - En fonction du règlement de travail, application de la CCT n° 81, du moins au personnel contractuel

## 3. Application ratione materiae de la CCT n° 81



- Encadre le contrôle des « données de communication électroniques en réseau »
  - E-mail
  - Internet / Intranet / Extranet
  - Sms, chat, forums de discussion, Wap...
- Ne s'applique pas aux modalités d'utilisation et/ou d'accès aux ressources informatiques => Liberté de l'employeur

## 4. Les modalités du contrôle



- Contrôle = permis mais sans atteinte excessive à la vie privée et aux libertés individuelles ou collectives
- Conditions :
  - Principe de finalité
  - Principe de proportionnalité
  - Principe de transparence
- Procédures d'individualisation : directe ou indirecte

## Principe de finalité



- 4 situations dans lesquelles le contrôle est permis :

- Prévention de faits illicites ou diffamatoires, contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui
- Protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires

Par exemple : contrôle pour prévenir des actes de piratage, consultation de sites pornographiques, pédophiles ou incitant à la haine raciale

Par exemple : contrôle pour prévenir de la publicité dénigrante, la divulgation de fichiers, de secrets d'affaires ou d'informations confidentielles

- La sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise

**Par exemple** : contrôle en cas de téléchargements de fichiers de tailles importantes et qui ralentissent le réseau ou présentant un risque d'infection par virus

- Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise

**Par exemple** : contrôle pour vérifier que les règles fixées pour l'accès et l'utilisation des ressources informatiques sont bien respectées

- Énumération exhaustive des finalités = le contrôle doit poursuivre un but précis

## Principe de proportionnalité



- Le contrôle ne peut entraîner une ingérence dans la vie privée du travailleur
- Si il y a une ingérence, elle doit être réduite au minimum

⇒ Le contrôle doit être adéquat, pertinent, non excessif et nécessaire au regard des finalités poursuivies

⇒ Il ne porte, dans un premier temps, que sur des données globales

⇒ Commission vie privée : contrôle temporaire et motivé par des soupçons. CCT ne précise pas.

## Principe de transparence

### • Information des travailleurs

- Information collective (conseil d'entreprise, délégués syndicaux...):
  - Politique de contrôle et prérogatives de l'employeur et du personnel surveillant
  - Finalités poursuivies
  - Conservation ou non de données à caractère personnel, le lieu et la durée de conservation
  - Caractère permanent ou non du contrôle
- Information individuelle (support au choix, règlement de travail, charte d'utilisation ...):
  - Utilisation de l'outil mis à la disposition du travailleur + limites fonctionnelles
  - Droits, devoirs et obligations des travailleurs + interdictions éventuelles quant à l'usage des moyens de communication électroniques en réseau
  - Sanctions prévues au règlement de travail en cas de manquement



## Procédures d'individualisation

But : analyser les données globales en vue de retracer l'identité de l'auteur de l'anomalie

- Principes :
  - En cas d'anomalie lors du contrôle
  - Individualisation des données de communication, PAS du contenu (sauf accord du travailleur)
  - Exception : consultation du contenu si caractère professionnel non contesté
  - L'individualisation sera directe ou indirecte selon les finalités poursuivies par le contrôle



### Individualisation directe

Identification immédiate du travailleur responsable de l'anomalie, sans formalité, lorsque les finalités du contrôle sont :

- prévention de faits illicites
- Protection des intérêts de l'entreprise
- Sécurité ou bon fonctionnement technique

### Individualisation indirecte

- Si le contrôle vise à s'assurer du respect de bonne foi des règles d'utilisation des technologies
- Phase préalable d'information collective
- Si récidive, individualisation directe
- Entretien individuel
- Sanctions, le cas échéant



## Dixième partie : Nouvelles technologies problématiques du point de vue de la vie privée



## 1. La technologie de radio-identification : RFID

- Appelé aussi smart-tag, radio-tag
- Ce sont de puces miniatures qui permettent par radio-diffusion de localiser et identifier un bien
- Utilisé pour :
  - Le profilage des individus
  - Le traçage des biens et des individus, la localisation de personnes/d'employés



### • Exemples

- Insertion de RFID dans des produits de consommation courantes : rasoirs Gillette
- Insertion sur des palettes de produits
- Dans des badges d'identification de personnes
- Dans des tickets d'avions
- Etc...



## Quid de la vie privée?



- Les RFID sont des données à caractère personnel = application de la LVP
- Il faut
  - Assurer l'information des personnes concernées!
  - Permettre le droit d'accès aux données
  - Protéger les données par des mesures techniques et organisationnelles
  - Permettre la neutralisation du RFID
- > difficultés pratiques



Etienne Wéry  
Avocat aux barreaux de Bruxelles et Paris  
Associé ULYS  
[www.uly.net](http://www.uly.net)