# Droit des TIC

## Partie 2:
Vie privée
et surveillance des travailleurs

Franck Dumortier
Franck.dumortier@unamur.be

# Introduction

- ✓ Les lieux de travail sont de + en + informatisés.

- ✓ L'employeur met à disposition du travailleur des outils de travail:

  - Ordinateur et autres supports de stockage
  - Réseau
  - Internet
  - Courrier électronique

➡ L'employeur peut-il contrôler l'usage de ces outils de travail, et si oui comment ?

# Introduction



## ✓ Loi du 3 juillet 1978 relative aux contrats de travail:

- Art 2 et 3: « *Le contrat de travail est le contrat par lequel un travailleur, s'engage contre rémunération à fournir un travail sous l'autorité (...) d'un employeur* ».

- Le lien de subordination du travailleur relève de l'essence même du contrat de travail.

➡ Un employeur doit-il pouvoir vérifier si le travail est effectué correctement et si les instructions données sont respectées ?

# Introduction



## ✓ Loi du 3 juillet 1978 relative aux contrats de travail:

- Art. 16. « *L'employeur et le travailleur se doivent le respect et des égards mutuels. Ils sont tenus d'assurer et d'observer le respect des convenances et des bonnes mœurs pendant l'exécution du contrat* ».

- Cette disposition s'applique également aux courriers électroniques ainsi qu'aux contenus visités/téléchargés.

- Voir également **l'art. 17 au slide suivant**

# Introduction



## ✓ Loi du 3 juillet 1978 relative aux contrats de travail:

- Art. 17. « *Le travailleur a l'obligation:*

*1° d'exécuter son travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus;*

*2° d'agir conformément aux ordres et aux instructions qui lui sont données par l'employeur […], en vue de l'exécution du contrat;*

*3° de s'abstenir, tant au cours du contrat qu'après la cessation de celui-ci :*

*a) de divulguer les secrets de fabrication, ou d'affaires, ainsi que le secret de toute affaire à caractère personnel ou confidentiel dont il aurait eu connaissance dans l'exercice de son activité professionnelle;*

*b) de se livrer ou de coopérer à tout acte de concurrence déloyale;*

*4° de s'abstenir de tout ce qui pourrait nuire, soit à sa propre sécurité, soit à celle de ses compagnons, de l'employeur ou de tiers;*

*5° de restituer en bon état à l'employeur les instruments de travail et les matières premières restées sans emploi qui lui ont été confiés ».*

# Introduction

- ✓ **Surveillance des outils de communications sur le lieu du travail**
- ✓ **Un droit et un intérêt contradictoires ?**
  - Le travailleur a le droit au respect de sa vie privée
  - L'employeur a intérêt contrôler l'utilisation de l'outil informatique qu'il met à disposition de son travailleur dans l'entreprise.

➡ Comment la loi concilie-t-elle le droit du travailleur et l'intérêt de l'employeur ?

➡ Aucune « loi » ne prévoit expressément le contrôle des données des travailleurs par l'employeur

# Introduction

- ✓ Enjeu important: la preuve pour licenciement !
  - Pour le patron: recommandation d'obtenir une preuve licite
  - Pour le travailleur: réussir à contester une preuve permet parfois d'obtenir un préavis/indemnité…

→ Mais… illégalité de la preuve n'équivaut pas à irrecevabilité de la preuve. Dans son arrêt du 10 mars 2008, la Cour de cassation a accepté que les règles d'exclusion de la preuve pénale soient applicables en matière civile et sociale !

→ Ainsi, la Cour a décidé que sauf en cas de violation d'une formalité prescrite à peine de nullité, une telle preuve ne peut être écartée que si elle a été recueillie d'une manière qui est entachée d'un vice préjudiciable à sa crédibilité ou qui porte atteinte au droit à un procès équitable.

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

# 1. Le droit à la vie privée des travailleurs

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

# 1.1. L'article 8 CEDH applicable aux travailleurs

# Droit à la vie privée des travailleurs

- ✓ Article 8 CEDH:

§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 ».

# Droit et intérêt légitime

- Le principe: droit à la protection de la vie privée.

- Ingérence à des conditions très strictes (Art. 8, §2):
  - ✓ **prévue par la loi** (avec suffisamment de clarté, de précision)
  - ✓ **Nécessaire** dans une **société démocratique** (proportionnalité)
  - ✓ **Pour** un des buts légitimes dont **le bien-être économique du pays ou la protection des droits et libertés d'autrui**

**Ces objectifs ne sont pas des droits fondamentaux mais des intérêts légitimes qui justifient des ingérences dans le droit au respect de la vie privée**.

# Droit à la vie privée des travailleurs

- ✓ La Cour européenne des Droits de l'Homme a déjà confirmé dans plusieurs arrêts que **la protection de la vie privée**, telle que définie à l'article 8 de la CEDH, **s'applique également au sein d'une entreprise.**

- ✓ Voy. **Arrêt Copland c. Royaume-Uni** (lien): Plainte d'une enseignante dont le téléphone avait été mis sur écoute et l'utilisation de la messagerie électronique et d'Internet contrôlée par son employeur, sans aucun consentement préalable de la part de l'intéressée.

➡ La Cour a jugé que les appels téléphoniques, les courriers électroniques ou les informations relatives aux sites Internet consultés par un travailleur sont couverts par les notions de "vie privée" et de "correspondance" au sens de l'article 8 de la CEDH.

# Droit à la vie privée des travailleurs

- ✓ Selon la Cour, même le fait d'enregistrer des « données de trafic » des travailleurs est une ingérence au sens de l'art 8, §2 CEDH:

> Toujours selon la Cour, le fait que ce contrôle serait limité à un relevé des dates et heures des appels effectués, ainsi qu'à l'identification des numéros composés importe peu. La Cour juge ici que cela est contraire à la CEDH, notamment vu l'absence de toute législation régulant de telles pratiques, mais elle ajoute que si une telle législation avait existé, un contrôle aurait été permis s'il avait été nécessaire dans une société démocratique, et ce "dans certaines situations". En tout cas, au regard de l'arrêt *Copland*, il est clair que l'affirmation selon laquelle il n'est plus question de protection de la vie privée dès que l'on se trouve sur le lieu de travail et que l'on utilise les équipements de l'employeur n'est pas défendable.

# Droit à la vie privée des travailleurs

- ✓ Ingérences dans la vie privée du travailleur possibles uniquement en vertu de l'art. 8, §2:

24. La Cour européenne a déjà précisé dans l'arrêt *Copland* qu'une restriction était en effet possible sous certaines conditions. On peut notamment déduire du texte de l'article 8 de la CEDH qu'une violation du droit au respect de la vie privée est permise lorsque les conditions suivantes sont remplies :

- la violation (est conforme à une norme existante, claire et accessible (*principe de légalité*) ;
- l'employeur doit avoir une finalité légitime, à savoir la nécessité de protéger un droit fondamental (*principe de finalité*);
- la violation doit être proportionnelle (*principe de proportionnalité*) : une violation du droit au respect de la vie privée n'est permise que si celle-ci est liée aux finalités pour lesquelles elle a été commise. Dans le cadre de ce contrôle de proportionnalité, le droit au respect de la vie privée peut être mis en balance non seulement avec d'autres droits fondamentaux, mais également, selon HENDRICKX et J.-F. NEVEN, avec les intérêts économiques de l'employeur[4].

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

# 1.2. Les dispositions belges applicables à la vie privée des travailleurs

# Droit à la vie privée des travailleurs

- ✓ Article 22 de la Constitution:« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. »
  - Applicable aux travailleurs
  - Attention ! Pour que l'ingérence en droit belge soit légale, il faut une loi au sens strict !
  - La loi au sens strict est l'acte posé par le pouvoir législatif fédéral. Il faut assimiler à la loi au sens strict les décrets adoptés par les Communautés et les Régions ainsi que les ordonnances de la région de Bruxelles-Capitale.

➡ Un Arrêté royal (acte posé par le pouvoir exécutif) ne suffit pas

# Droit à la vie privée des travailleurs

- ✓ **La loi belge du 8 décembre 1992 relative à la protection des données à caractère personnel est applicable aux travailleurs.**

- ✓ **Les obligations du responsable du traitement :**

1. Déclaration à la Commission vie privée **(ATTENTION ! Supprimé dans le GDPR);**
2. Information;
3. Sécurité.

- ✓ **Droits de la personne concernée:**

1. Droit d'accès :
   - recevoir (sur demande) copie des données la concernant
   - demander au responsable s'il détient des données la concernant, lesquelles et pourquoi et à qui elles sont transférées
2. Droit de rectification des données inexactes la concernant
3. Droit de suppression de données inexactes, incomplètes ou non pertinentes
4. Droit d'opposition

# Droit à la vie privée des travailleurs

## Pour le futur, art. 88 GDPR:

*Traitement de données dans le cadre des relations de travail*

Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.

# Droit à la vie privée des travailleurs

- ✓ Le principe de **confidentialité du contenu des communications** s'appliquent aux travailleurs

- **Art. 314bis du Code Pénal**: *« § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, quiconque : 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications; 2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque ».*

➡ Cette disposition ne concerne que le contenu des communications, à l'exclusion des données de trafic/données de communication

# Droit à la vie privée des travailleurs

- ✓ Le principe de **confidentialité des données de trafic** s'appliquent aux travailleurs

- ✓ **Art. 124 de la LCE du 13 juin 2005:** *« S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :*

  *1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement;*

  *2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;*

  *3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives a une autre personne;*

  *4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non ».*

# Droit à la vie privée des travailleurs

- ✓ Pour rappel: L'article 550bis, §2 du Code pénal incrimine la personne qui outrepasse son pouvoir d'accès à un système informatique de manière frauduleuse ou dans le but de nuire.

- ✓ En cas de violation, l'employeur risque un emprisonnement de six mois à deux ans et une amende de vingt-six euros à vingt-cinq mille euros ou d' une de ces peines seulement

- ✓ Dès lors, comment l'employeur peut-il procéder à:
  - la journalisation des données de trafic ?
  - l'accès aux données journalisées ?
  - l'accès au contenu des dossiers/fichiers/e-mails ?

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

# 2. La journalisation (rétention) des données de trafic des travailleurs

# Journalisation des données des travailleurs

- ✓ Exceptions à la confidentialité des communications : art. 125 de la LCE du 13 juin 2005

*« 1er. Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables :*
*1° lorsque la loi permet ou impose l'accomplissement des actes visés;*
*2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques […]»*

Pour porter atteinte à la confidentialité du contenu et des données de trafic du travailleur, il faut:

- Une loi au sens strict
- OU Assurer la sécurité d'un réseau (mais de manière proportionnée)

# Journalisation des données des travailleurs

- ✓ La question se pose de savoir si la loi du 3 juillet 1978 relative aux contrats de travail peut constituer une base légale suffisante pour justifier une ingérence dans l'article 314bis du Code pénal et à l'article 124 de la LCE.

- ✓ Selon les art. 16 et 17 de cette loi, l'employeur dispose d'un droit de contrôle à l'égard des prestations fournies sous son autorité et de l'obligation d'observer et de faire observer les convenances.

- ✓ Certains auteurs prétendent que ces dispositions ne sont pas suffisamment précises pour servir de fondement légal, une partie importante de la jurisprudence et la Commission Vie Privée considèrent toutefois que ces dispositions peuvent effectivement servir de fondement légal.

➡ **Plus rigoureux, selon moi, de fonder la légalité de la journalisation des données de trafic (mais pas l'accès) sur l'art. 16, §4 de la loi du 8 décembre 1992.**

# Journalisation des données des travailleurs

- ✓ **Art. 16, §4 de la loi du 8 décembre 1992 :**

*« Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels (…) »*

# Journalisation des données des travailleurs

- Obligation de tout « responsable du traitement » de prendre les mesures techniques et organisationnelles requises pour protéger les données (sécurité):
    - En tenant compte de l'état de la technique,
    - des frais
    - des risques
    - et de la nature des données à protéger

# Journalisation des données des travailleurs

- **L'obligation de sécurité selon la CPVP:** Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel (voir ici)

➡ Mesures de référence inspirées de la norme ISO 27002

- Voir aussi les Lignes directrices pour la sécurité de l'information (disponibles ici)

# Journalisation des données des travailleurs

- Selon la CPVP, « dans le contexte normatif », la sécurité de l'information implique la préservation de 7 caractéristiques de la sécurité:

  - la confidentialité,
  - l'intégrité,
  - la disponibilité,
  - **l'imputabilité (!)**,
  - l'authenticité,
  - la fiabilité
  - et la non répudiation

# Journalisation des données des travailleurs

✓ La CPVP définit l'imputabilité comme étant:

*« la propriété qui garantit que les actions d'une entité sont tracées et attribuées à cette seule entité. L'imputabilité assure de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) »*

➡ Recommandation de conserver des « logs »

# Journalisation des données des travailleurs

- ✓ Mesures de références CPVP:

**7. Journalisation, traçage et analyse des accès**

**L'organisme doit mettre en œuvre des mécanismes de journalisation et de traçage.**

Ces derniers doivent permettre de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci. L'enregistrement de ces informations de contrôle peut concerner, suivant les cas, l'accès physique, l'accès logique ou les deux.

La granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte. Des mécanismes supplémentaires de détection d'intrusion pourraient être requis. Le conseiller en sécurité de l'information doit être en mesure de justifier la politique adoptée.

Les données de traçage étant elles-mêmes des données à caractère personnel, tout traitement de celles-ci doit s'accompagner des mesures de sécurité adéquates.

# Journalisation des données des travailleurs

- ✓ Pour ce qui concerne l'enregistrement de logs de connexion des travailleurs, l'article 16, §4 de la loi de '92 suffit.

- ✓ Attention ! L'enregistrement de logs étant considérés comme un traitement de données à caractère personnel, les règles de la loi de '92 s'appliquent (en particulier l'obligation d'information, de délai de conservation raisonnable, de droit d'accès par le travailleur, sécurité etc).

- ✓ Mais quid de l'accès aux logs par l'employeur ?

➡ Cette question a été négociée par le biais de la Convention collective de travail n°81

# 3. La convention collective de travail n°81 du 26 avril 2002

# La CCT n°81

- Le 26 avril 2002, la convention collective de travail n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau a été signée au sein du Conseil national du Travail. (lien)

- Cette CCT 81 organise les différents principes de finalité, de proportionnalité et de transparence, applicables lorsqu'un employeur décide de mettre en place un système de contrôle portant sur les données électroniques en réseau.

- Cette CCT 81 a été rendue obligatoire dans le secteur privé par Arrêté royal (lien)

- Même si cette CCT ne s'applique pas au secteur public, les employeurs de ce secteur ne peuvent pas passer outre à la CCT n° 81 car elle constitue une spécification de la loi vie privée qui leur est bel et bien applicable.

# La CCT n°81

1. La CCT règle le contrôle de l'utilisation du réseau et le contrôle de l'utilisation des moyens de communications.

   ➡ Application de la CCT n°81 (concerne les données de trafic mais pas le contenu des communications)

2. La CCT ne règle pas le contrôle du contenu des données électroniques.

   ➡ En principe, interdit : sauf ingérence proportionnelle sur base de la loi du 8 décembre 1992

# La CCT n°81

La CCT n°81 règle:

- ✓ Quel usage le travailleur ne peut-il pas faire des moyens de communications ?

  ➡ Par ce biais, la CCT indique pour quelles finalités un contrôle est possible.

- ✓ Quel contrôle l'employeur peut-il exercer sur l'usage que son travailleur fait de ces moyens ?

  ➡ La CCT indique les conditions et procédures à respecter pour un contrôle des données de trafic par l'employeur.

UNIVERSITÉ DE NAMUR

# Quel usage le travailleur peut-il faire des moyens de communication?

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

1. Rien d'illégal :

   - Consultation de sites illicites (ex: pédophilie, drogues, armement, racisme, etc.)
   - Cybercriminalité : hacking, fraude informatique, etc.
   - Envoi de messages qui peuvent nuire à des tiers ou à l'employeur

# Quel usage le travailleur peut-il faire des moyens de communication ?

2. Pour le reste, l'employeur détermine l'usage qui peut en être fait (par ex dans le Règlement de travail).

- Interdire l'utilisation de l'e-mail à ou du web des fins privées
- Conditionner cette utilisation :
  - Uniquement en dehors des heures de travail, à titre occasionnel
  - Indiquer le caractère privé du message (SUJET : privé)
  - supprimer, dans le corps du message, toute mention relative à l'employeur (p. ex. la signature automatique de l'employeur) Interdire d'envoyer ou de recevoir des fichiers d'une taille supérieure à x Ko
  - Interdit de forwarder des e-mails en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice à l'employeur ou à l'auteur du message originel
  - Interdit de surfer sur des sites pornos, etc.
  - L'employeur se réserve le droit de bloquer l'accès à des sites web.
  - Autoriser ou interdire l'usage de TOR

# Exemple (1)

## Utilisation du téléphone fixe et du GSM communal

Article 174

L'agent veillera à utiliser le téléphone fixe ainsi que le GSM mis à sa disposition sur le lieu de travail pour des appels liés à l'exercice de sa fonction;

L'utilisation du téléphone fixe à des fins privées devra obligatoirement se faire via le code prévu à cet effet à savoir *745566;

Les communications privées seront limitées aux appels nécessaires et ne pourront en aucun cas porter atteinte à la qualité et à la quantité de travail à fournir;

Elles s'effectueront de préférence durant les temps de pause;

L'utilisation du GSM à des fins privées est interdite;

Les communications abusives ou privées pourront faire l'objet d'une refacturation à l'agent;

# Exemple (2)

## Utilisation d'Internet

### *Utilisation d'internet et de la messagerie électronique « @ixelles.be » à des fins professionnelles*

Article 176

Durant son temps de travail, l'agent veillera à utiliser internet et sa messagerie électronique « @ixelles.be » exclusivement à des fins professionnelles.

### *Utilisation d'internet et de la messagerie électronique « @ixelles.be » à des fins privées*

Article 177

L'utilisation d'internet et de la messagerie électronique « @ixelles.be » à des fins privées est autorisée uniquement durant les temps de pause.

Dans son utilisation d'internet, il est strictement interdit à l'agent :

- d'envoyer des messages ou de consulter des sites dont le contenu est susceptible de porter atteinte à la dignité d'autrui ;
- de consulter des sites à caractère érotique ou pornographique.

UNIVERSITÉ DE NAMUR

# Quel contrôle l'employeur peut-il exercer ?

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Trois grands principes à respecter lors du contrôle :

1. Principe de finalité
2. Principe de transparence
3. Principe de proportionnalité

UNIVERSITÉ DE NAMUR

# CCT n°81
## 1) Principe de finalité

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Article 5

§ 1er. Le contrôle de données de communication électroniques en réseau n'est autorisé que lorsque l'une ou plusieurs des finalités suivantes est ou sont poursuivies :

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;

2° la 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 ;

3° 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 ;

4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

PAS de contrôle SECRET !

Il faut fournir une information sur le contrôle

# CCT n°81
# 2) Principe de transparence

1) Information collective

Article 7

§ 1er. L'employeur qui souhaite installer un système de contrôle des données de communication électroniques en réseau, informe le conseil d'entreprise sur tous les aspects du contrôle visés à l'article 9, § 1er de la présente convention, conformément aux dispositions de la convention collective de travail n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise.

§ 2. A défaut de conseil d'entreprise, cette information est fournie au comité pour la prévention et la protection au travail ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs.

2) Information individuelle

Article 8

§ 1er. Lors de l'installation du système de contrôle des données de communication électroniques en réseau, l'employeur informe les travailleurs concernés sur tous les aspects du contrôle visés à l'article 9, §§ 1er et 2.

§ 2. L'information fournie est effective, compréhensible et mise à jour. Le choix de son support est laissé à l'employeur.

§ 3. Cette information ne dispense pas les parties de respecter le principe d'exécution de bonne foi des conventions.

## Comment fournir l'information ?

- ✓ Information collective des travailleurs (conseil d'entreprise, délégation syndicale…)

**ET**

- ✓ Information individuelle
  - règlement de travail,
  - mention dans le contrat de travail
  - message d'avertissement à chaque utilisation de l'outil

## Informations à fournir :

- politique de contrôle et prérogatives de l'employeur et du personnel surveillant
- Finalité(s) poursuivie(s)
- Le fait que les données personnelles sont conservées (durée et lieu de conservation)
- Caractère permanent ou non du contrôle
- Utilisation de l'outil et limites à cette utilisation
- Interdictions éventuelles prévues dans l'utilisation
- Droits et obligations des travailleurs
- Sanctions prévues par le règlement de travail en cas de manquement

# CCT n°81
# 3) Principe de proportionnalité

- ✓ Pas de surveillance générale, permanente et *a priori* de l'usage fait par un travailleur en particulier

- ✓ Contrôle ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail

Article 6

Par principe, le contrôle des données de communication électroniques en réseau ne peut entraîner une ingérence dans la vie privée du travailleur.

Si toutefois ce contrôle entraîne une ingérence dans la vie privée du travailleur, cette ingérence doit être réduite à un minimum.

# CCT n°81
# 3) Principe de proportionnalité

- ✓ A quelles données l'employeur peut-il avoir accès ?

  A priori, seules des données globales pourront dans un premier temps être récoltées, sans qu'un travailleur spécifique ne soit identifié.

  Ex : la durée de connexion à internet et le nombre et volume de messages électroniques envoyés en général

- ✓ Quid de l'individualisation ?

  L'individualisation des données de communication électroniques en réseau est l'opération consistant à traiter des données globales collectées en vue de les attribuer à un travailleur identifié ou identifiable.

- ✓ Il y a deux types d'individualisation, **l'individualisation directe et indirecte.**

# Que peut faire l'employeur s'il détecte une anomalie ?

## 1) Anomalie détectée dans le cadre des finalités suivantes :

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;

2° la 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 ;

3° 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 ;

➡ L'employeur **peut directement identifier l'auteur**

NB: >< à l'art 125 LCE qui exige une loi au sens strict: la CCT n°81 n'est rendue obligatoire que par Arrêté royal.

# Que peut faire l'employeur s'il détecte une anomalie ?

## 2) Anomalie détectée dans le cadre de la finalité suivante:

4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

➡ procédure de « sonnette d'alarme »: **identification indirecte**

- ✓ Information collective des travailleurs

  Ex. : avertissement par e-mail collectif

- ✓ Si le problème persiste : identification de l'auteur

  Entretien au cours duquel il pourra s'expliquer, émettre des objections (possibilité de se faire assister par délégué syndical)

# 4.

# L’accès par l’employeur au contenu de communications/fichiers de travailleurs stockés dans l’outil de travail

# Accès aux données électroniques stockées

- ✓ La plupart des données générées par les outils de travail électroniques mis à disposition des travailleurs sont sauvegardées, voire même copiées sur un autre support à des fins de back-up (archivage).

- ✓ L'accès au contenu des courriers électroniques/dossiers des employés ne relève pas uniquement d'une question de surveillance…

- ✓ mais peut également servir à assurer la continuité du service en cas

  - d'absence,
  - de départ/licenciement,
  - ou de décès du travailleur.

# Contrôle des données électroniques stockées

- ✓ Sur quelle base juridique l'employeur peut-il avoir accès au contenu ?

- ✓ Pour les données stockées: difficile d'appliquer la confidentialité des communications électroniques (art. 124 LCE et 314bis CP non-applicables)

- ✓ Libre accès ? Non

  - Etat de nécessité (empêcher ou stopper une infraction)
  - **Application de la loi du 8 décembre 1992: Finalité + Proportionnalité + Transparence**

# Contrôle des données électroniques stockées

- ✓ La LVP s'applique à « tout traitement de données à caractère personnel automatisé en tout ou en partie »

  Le contenu des messages électroniques envoyés ou reçus à une telle adresse (qu'ils revêtent ou non un caractère professionnel), sont des données à caractère personnel (idem pour fichiers/dossiers stockés)

- ✓ Par « traitement », on entend *« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »*

➡ **L'accès au contenu des messages/dossiers/fichiers du travailleur par l'employeur doit s'analyser comme un « traitement de données à caractère personnel ».**

# Contrôle des données électroniques stockées

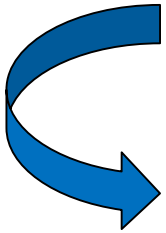
UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

✓ **Conséquence : application des principes de la LVP ! (1)**

- Principe de finalité déterminée : assurer une continuité des services prestés en cas d'absence, de décès du travailleur ou de départ de celui-ci de l'entreprise, de conserver des documents à des fins de preuve, ou encore un contrôle

- Principe de finalité légitime: Le consentement du ou des travailleurs concernés ne peut constituer la base légale autorisant le contrôle patronal vu le rapport de forces



Fondement dans l'exécution des contrats de travail, vu la nature de ce contrat (article 5, b) de la LVP) ou poursuite d'un intérêt légitime de l'employeur (article 5, f) de la LVP).

# Contrôle des données électroniques stockées

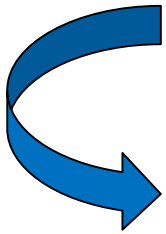
UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

## ✓ Conséquence : application des principes de la LVP ! (2)

- Principe de proportionnalité: L'objectif spécifique poursuivi à l'occasion de l'accès doit répondre aux besoins ou aux règles de l'entreprise ou découler de la nature du contrat de travail ou de la tâche à exécuter + le traitement mis en œuvre doit s'avérer nécessaire pour atteindre cet objectif.

- Principe de qualité (minimisation) de l'accès: les données traitées à cette occasion doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.



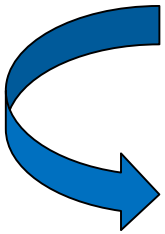
**En principe, aucune « nécessité » pour l'employeur d'avoir accès à des contenus d'ordre privé. Accès possible uniquement pour des contenus d'ordre professionnel.**

# Contrôle des données électroniques stockées

- ✓ **Conséquence : application des principes de la LVP ! (3)**

  - Principe de transparence: Obligation de fournir certaines informations aux travailleurs concernés notamment sur la finalité de traitement + déclarer le traitement préalablement à la Commission (disparait sous le GDPR)

  - L'employeur doit déterminer, dans la politique ou charte d'utilisation des outils ICT de son organisation, les conditions de consultation de la messagerie électronique professionnelle/ dossiers de son entreprise en cas d'absence de l'employé et ce, en concertation avec les travailleurs (conseil d'entreprise, comité de prévention pour la sécurité et le bien-être au travail, travailleurs).



**Importance de la charte ICT qui doit fixer des règles d'utilisation et des procédures d'accès par l'employeur.**

# Comment ?

- ✓ Voir recommandations de la CPVP relatives à la cyber-surveillance

À titre de recommandation générale de base, il convient d'élaborer au maximum des règles préventives (sur le plan juridique, en lien avec le management et sur le plan technique) ainsi que des procédures préventives (par exemple pour le classement d'e-mails, de documents, de fichiers) afin d'éviter que survienne le besoin dans le chef de l'employeur de contrôler et d'accéder à des informations personnelles des travailleurs.

Les travailleurs ont certes le droit d'effectuer des communications privées sur le lieu de travail, dans une mesure limitée, mais pour protéger leur vie privée, mieux vaut séparer autant que possible les e-mails professionnels des e-mails privés.

Les e-mails privés reçus ou envoyés pendant les heures de travail par le travailleur ne sont en effet *a priori* pas destinés à être lus ou reçus par l'employeur, et certainement pas en ce qui concerne leur contenu[1].

Les e-mails fonctionnels doivent par contre *a priori* pouvoir être traités dans le contexte normal de communication professionnelle au sein d'une entreprise/administration publique – et il en va de même en ce qui concerne leur contenu -, étant donné qu'ils concernent évidemment l'exécution de la tâche de travail au sens strict.

En cas de double utilisation du système d'e-mails, il est toutefois difficile de concilier les droits et intérêts des deux parties.

# Comment ?

Pratique n°1 : Séparer le privé du professionnel

1. Pour les informations, fichiers et documents

Exemple 1 : Stockage des informations privées

- Création sur le poste de travail d'un répertoire nommé "Privé-Nom de l'utilisateur" servant à stocker tous les documents non professionnels, répertoire ne pouvant contenir des informations professionnelles.

- Le répertoire privé est placé sur une partition du disque dur ne faisant pas l'objet de copies de sécurité (back-up) centralisées et systématiques.

Exemple 2 : Stockage des informations professionnelles

- Les informations professionnelles, à l'exclusion de toute information privée, sont obligatoirement stockées sur le disque dur d'un serveur central, le cas échéant dans des répertoires réservés à l'utilisateur. Les documents professionnels sur le poste de travail n'étant que des copies, à considérer comme temporaires et ne faisant pas nécessairement l'objet de copies de sécurité systématiques (celles-ci se faisant centralement pour les informations du serveur).

# Comment ?

2. Pour les messages électroniques

Exemple 3 : Stockage des informations privées

- Création dans la boîte de messagerie d'un répertoire nommé "Privé-Nom de l'utilisateur" servant à stocker tous les messages non professionnels (envoyés et reçus), répertoire ne pouvant contenir des messages professionnels (les cas de non-respect pouvant faire l'objet de sanctions).

Exemple 4 : Utilisation de comptes distincts

- Attribution de deux (ou plus) comptes de messagerie avec des identifiants distincts pour chaque utilisateur, l'un pour la messagerie privée, les autres pour la messagerie professionnelle selon le type d'activité. Cette distinction peut se faire par le nom (exemple : initiales@domaine.com pour le professionnel et nom.prénom@domaine.com pour le privé) ou par le nom de domaine (par exemple : nom@domaine.com pour le professionnel et nom@domaine.net pour le privé), ou encore, via un sous-domaine du type nom@domaine.personnel.com.

# Comment ?

Pratique n°2 : Exclure des activités certaines opérations dangereuses

Pour garantir le respect de certaines instructions d'utilisation des outils informatiques et éviter une surveillance qui donnerait accès à des informations sans utilité pour l'employeur, il peut être opportun d'empêcher certaines opérations via les outils de l'entreprise (par exemple, bloquer l'accès à certains sites ou de bloquer certaines adresses électroniques reconnues comme dangereuses) ou de programmer des messages d'alerte réservés à l'utilisateur en cas d'opérations suspectes. Les différentes fonctions et listes de sites et d'adresses d'expéditeurs à interdire sont proposées dans les logiciels spécifiques (suites de sécurité Internet) et peuvent être complétées par les besoins spécifiques de l'entreprise.

# Comment ?

Pratique n°3 : L'accès aux communications personnelles exige un encadrement spécifique

Certaines communications professionnelles peuvent avoir un caractère spécifiquement personnel (par exemple par une mention dans l'objet). L'accès au contenu de ces communications, mêmes si elles sont clairement professionnelles, ne pourra se faire qu'avec la prudence appropriée.

Exemple 1 :

- Indication "PERSONNEL" ou "CONFIDENTIEL" dans l'objet du message. Toutefois, il semble difficile d'obtenir cette discipline pour les tiers envoyant des messages à l'entreprise.

Exemple 2 :

- Utilisation de répertoires spécifiques, au sein des espaces réservés aux informations professionnelles

Exemple 3 :

- Pour sélectionner les messages et leur donner la fin nécessaire, on désignera une personne de confiance, neutre, soumise au devoir de confidentialité et habilitée à apprécier la qualité du message. Ce n'est qu'exceptionnellement qu'un supérieur hiérarchique, un collègue ou un assistant administratif sera la personne appropriée.

# Comment ?

- En cas de départ avec prestation du préavis, prévoir une procédure analogue à celle prévue pour les absences planifiées du travailleur, le cas échéant en concertation avec le travailleur au moment du départ.

- En cas de départ sans prestation du préavis, une personne est désignée au cas par cas, en vertu d'un accord mutuel entre l'employeur et un représentant du personnel ; cette personne étant habilitée à gérer les messages entrants au nom du travailleur.

- Prévoir dans la politique de sécurité de l'information la suite à réserver aux messages professionnels (transfert à un autre travailleur approprié) et aux messages privés (effacement ou transfert vers une adresse privée pendant une durée limitée d'1 mois). Il n'est pas toujours recommandé d'indiquer dans le message automatique de réponse à l'expéditeur que le travailleur ne fait plus partie du personnel de l'organisme ; une telle indication ne pourra donc se faire qu'avec le consentement explicite et formel du travailleur.

- Prévoir dans la politique de sécurité de l'information la suite à réserver aux fichiers et informations à caractère privé (les fichiers et informations professionnels pouvant être utilisés par l'employeur conformément aux règles internes).

UNIVERSITÉ DE NAMUR

# Comment ?

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

**Encadrez les opérations de surveillance et de contrôle**

- à l'occasion d'un accès à des données de communication électroniques, que ce soit dans le cadre d'un contrôle ou non, ne traitez que des données à caractère personnel adéquates, pertinentes, exactes et actualisées. Ces données ne peuvent pas être conservées pour une durée supérieure à celle nécessaire à la réalisation de la finalité ;

- veillez à ce que la personne chargée de la recherche et de la collecte de données à caractère personnel soit une autre personne que celle qui en donne l'ordre ;

- veillez à ce que la personne chargée de la recherche agisse sur la base d'instructions les plus précises possibles, formulées par le demandeur, et qu'elle se limite, dans sa recherche, à ce qui lui a été demandé ;

- veillez à ce que la recherche se fasse autant que possible sur la base de critères pertinents qui permettent dans un premier temps d'exclure de la consultation un maximum d'informations ;

- veillez à ce que la recherche ait lieu avant tout sur la base de dates, de mots clés, de l'identité des destinataires ou des expéditeurs de messages avant d'accéder à leur contenu ;

- édictez des règles spécifiques en matière d'accès et d'utilisation pour le gestionnaire du système dans le cadre de l'exercice de sa fonction ;

# Comment ?

- ne prenez pas de décision importante à l'encontre de la personne concernée simplement sur la base d'informations collectées dans le cadre d'un traitement de ses données à caractère personnel (par exemple dans le cadre d'une opération de surveillance ou de contrôle) ;

- avant de prendre une quelconque décision à l'encontre de la personne concernée, offrez-lui la possibilité de faire valoir son point de vue, notamment quant à l'exactitude et à la pertinence des données à caractère personnel collectées.

# Comment ?

**Garantissez le respect des règles et renforcez la sécurité de la surveillance et du contrôle**

- conservez un relevé écrit de l'ensemble des opérations constituant une intrusion dans les outils informatiques ou dans les informations qu'ils génèrent (ce qui a été consulté, collecté et transmis, quand, comment, pour le compte de qui, et par qui et à qui ces informations ont été communiquées) pour permettre tout contrôle du respect, par l'employeur, du principe de finalité et du principe de proportionnalité ;

- si la gestion et la maintenance des outils et des réseaux est réalisée par un prestataire externe, veillez à ce que les règles internes d'entreprise s'appliquent également à ce prestataire et concluez un contrat de sous-traitance avec un tel prestataire ;

- soumettez l'organisation des procédures mais aussi les opérations de surveillance et de contrôle concrètement envisagées, et de manière plus générale tous les accès aux outils informatiques, si disponibles, au préposé à la protection des données de l'entreprise afin qu'il puisse en apprécier le caractère nécessaire et licite ;

Franck Dumortier
Chercheur
Centre de Recherche Information, Droit et Société (CRIDS)
franck.dumortier@unamur.be
www.crids.eu