

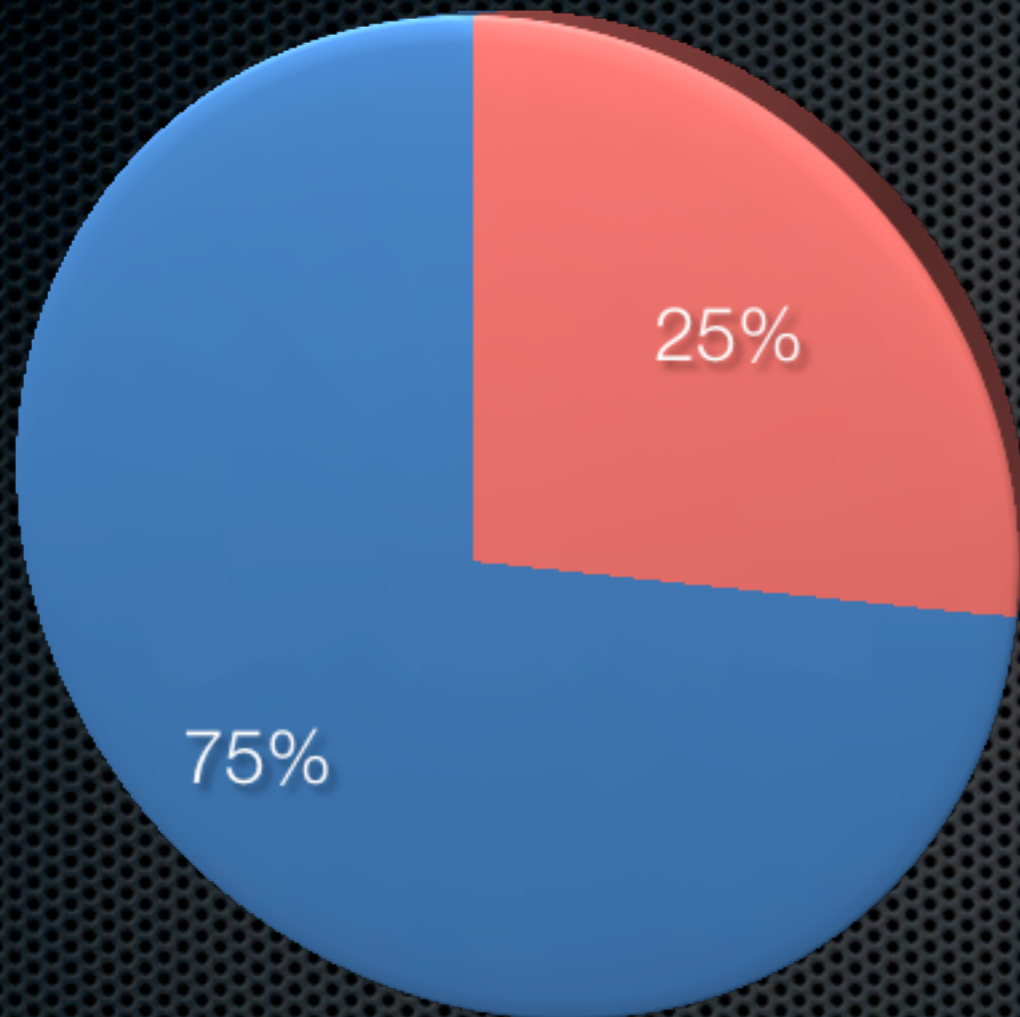
Accès distants au SI

Besoins métier vs Besoins de sécurité,
comment faire arbitrer ?

Sommaire

- ✦ Les accès distants
- ✦ Les besoins métier
- ✦ Les menaces
- ✦ La démarche pour faire arbitrer

Les accès distants



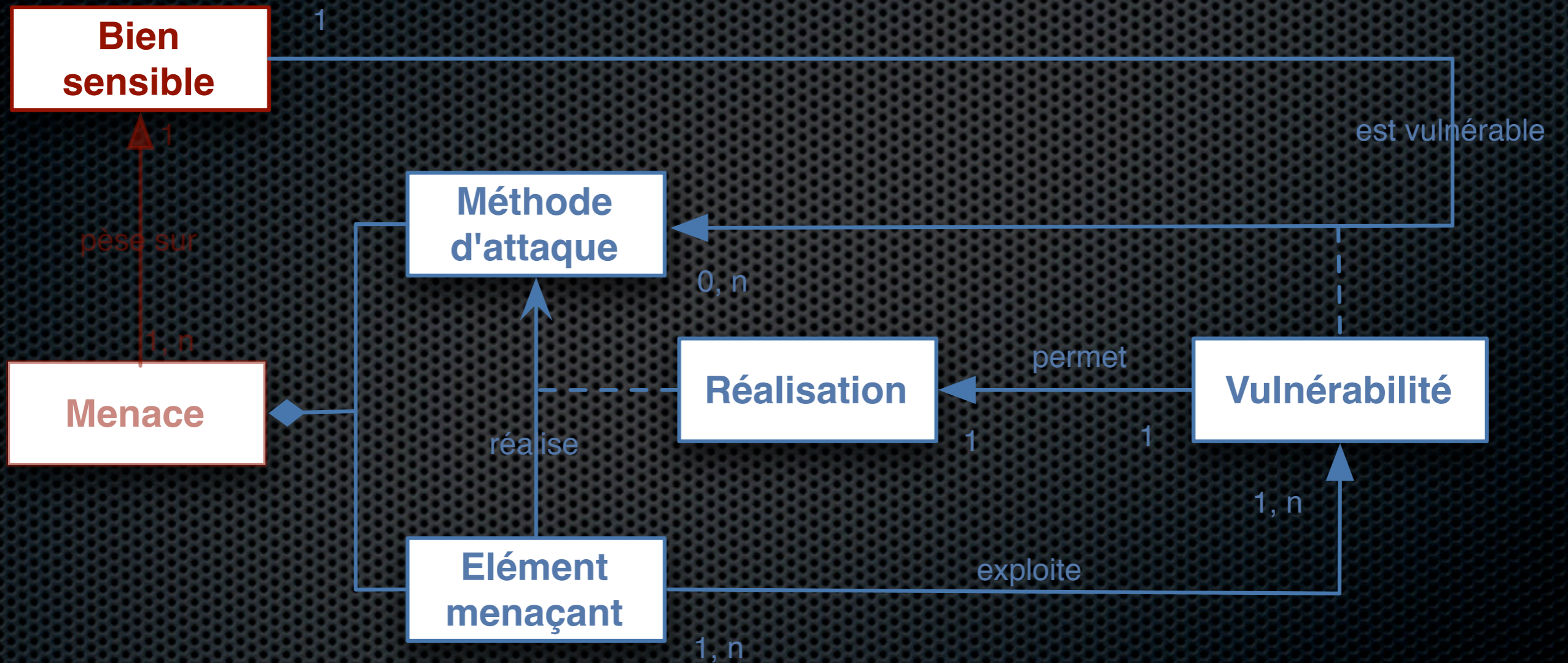
● Mobile = 878 Millions
● Fixe

At least 10 hours per week away from home and from their main place of work, ... use online computer connections when doing so.

Les besoins métier

- ✦ Déplacements plus fréquents
- ✦ Gagner en productivité
- ✦ Rapidité
- ✦ Réactivité

La menace



Méthodes d'attaque

- ✦ Espionnage à distance
- ✦ Interception des communications
- ✦ Vol de données
- ✦ Piégeage

Éléments menaçants

✦ Vecteurs

Agent

Technicien “opérateur”

Pirate

✦ Commanditaires

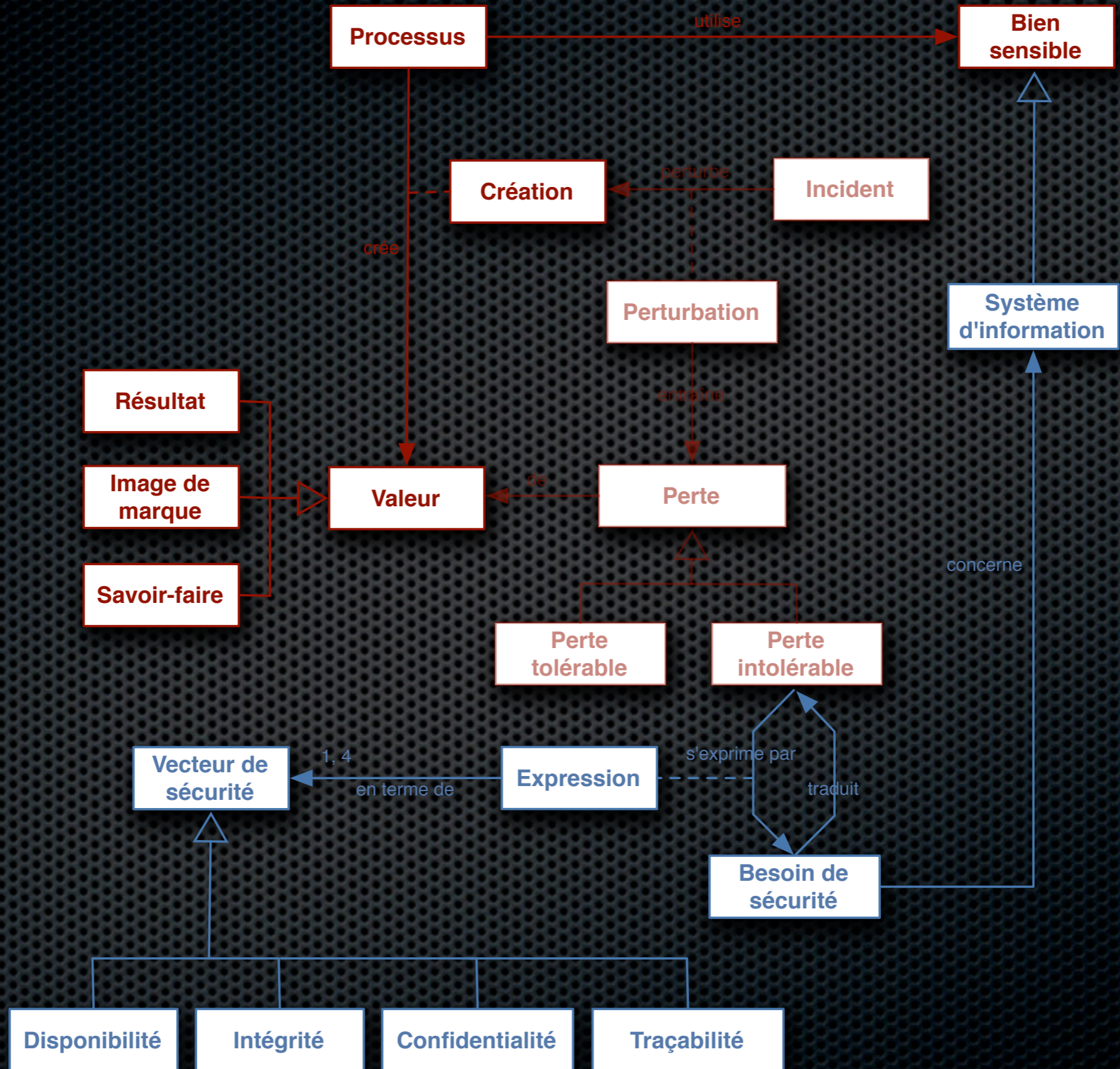
Agence

Société de renseignement

Organisation

La démarche pour faire arbitrer

1. Formaliser les besoins de sécurité du métier
2. Etudier les risques
3. Définir les mesures de sécurité
4. Sensibiliser





Définir les mesures de sécurité

- ✦ Répondre aux besoins de sécurité du métier
- ✦ Réduire les risques
- ✦ Limiter les contraintes

Sensibiliser

- ✦ Présenter les mesures

les biens qu'elles protègent

contre quels risques

comment et avec quelles contraintes

Cybersurveillance des salariés et contraintes juridiques

Me Jean-Philippe LECLERE
Avocat

Introduction

➤ Les moyens « classiques » de surveillance

- ◆ Surveillance des communications téléphoniques (écoutes téléphoniques, autocommutateurs, usage des mobiles)
- ◆ Vidéosurveillance
- ◆ Badges d'accès

➤ Les moyens « modernes » de surveillance:

- ◆ Contrôle de l'utilisation d'Internet (surf, e-mails)
- ◆ Biométrie
- ◆ Géolocalisation
- ◆ Alerte éthique

Introduction

➤ Les risques pour les salariés

- ◆ Atteinte au respect de la vie privée
- ◆ Disproportion des méthodes de contrôle

➤ Les risques pour les employeurs:

- ◆ Intrusion, espionnage, atteinte aux biens, à l'image de l'entreprise
- ◆ Pertes de productivité
- ◆ Engagement de responsabilités civile et pénale

Introduction

Responsabilité civile de l'employeur :

Article 1384 alinéa 5 du Code Civil

Affaire « Escota » : site réalisé sur le SI de l'entreprise par un employé et injuriant une autre société

L'employeur a été jugé responsable car une note de service autorisait pour les salariés « la consultation d'autres sites que ceux présentant un intérêt direct en relation directe avec leur activité »

Introduction

Responsabilité pénale de l'employeur :

Article 121-1 L 121-7 du Code Pénal

Article L 121-3

Manquement à une obligation de prudence ou de sécurité prévue par la loi

Article L 121- 7

Complicité d'un crime ou d'un délit d'une personne qui en a sciemment facilité la préparation ou la préparation

Délégation pénale

Introduction

Problématique :

Trouver un équilibre entre :

- le pouvoir disciplinaire de l'employeur (pouvoir de contrôle de l'activité professionnelle de l'employé et pouvoir de sanction)
- le droit fondamental de la protection de la vie privée de l'employé y compris sur le lieu de travail

Les textes de référence

- **Loi du 6 janvier 1978 « Informatique et Libertés »**
- **Code du Travail**
- **Code Civil (Article 9)**
- **Code Pénal**
- **Loi du 10 juillet 1991 : secret des correspondances**

Le courrier électronique

➤ Statut juridique

Assimilation à une correspondance privée si le message est exclusivement destiné à une ou plusieurs personnes physiques déterminée(s) et individualisée(s).

Ne sont pas assimilés à des correspondances privées : newsletters, courriers non sollicités

➤ Application du principe du secret des correspondances (Article 226-15 C.P.)

- ♦ « Quiconque, de mauvaise foi, ouvre, supprime, retarde, détourne, utilise, divulgue des correspondances et en prend connaissance frauduleusement »
- ♦ Sanctions pénales (1 an d'emprisonnement, 45 000 € d'amende)

Le courrier électronique

➤ Problématique

- ♦ Le secret des correspondances s'applique t-il à l'ensemble des messages émis et reçus dans l'entreprise ?
- ♦ Doit-on faire une distinction entre les messages électroniques professionnels et privés et selon quels critères ?
- ♦ Quels sont les modalités du contrôle par l'employeur ?

Le contrôle de l'usage de la messagerie

Evolution de la jurisprudence :

- Arrêt « NIKON » du 2 octobre 2001: l'employeur ne peut prendre connaissance des messages personnels des salariés
- Arrêt du 17 mai 2005 : l'employeur ne peut prendre connaissance des messages personnels des salariés, hors sa présence si un risque ou un évènement le justifie
- Arrêts du 18 octobre 2006 : les dossiers et fichiers créés par un salarié dans l'entreprise sont présumés professionnels.
- Arrêt du 23 mai 2007: l'employeur peut dans certaines conditions accéder aux contenus des messages électroniques.

Le contrôle de l'usage de la messagerie

ARRET NIKON :

- le salarié a droit sur le lieu de travail au respect de l'intimité de sa vie privée
- le secret des correspondances s'applique à des messages classés dans un fichier « Personnel »
- *« l'employeur ne peut 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 telle utilisation »*

Le contrôle de l'usage de la messagerie

ARRET du 17 mai 2005 :

- Sont concernés des fichiers et non pas des messages qualifiés de « personnels » par le salarié et stockés sur son poste informatique
- *« 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 »*

Le contrôle de l'usage de la messagerie

ARRETS OCTOBRE 2006 :

Présomption du caractère professionnel des fichiers créés par le salarié.

- « les documents détenus par le salarié dans le bureau de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, présumés avoir un caractère professionnel, en sorte que l'employeur peut y avoir accès hors sa présence »
- « les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme personnels, présumés avoir un caractère professionnel, de sorte que l'employeur peut y avoir accès hors sa présence »

Le contrôle de l'usage de la messagerie

ARRET 23 MAI 2007 :

- L'employeur peut faire appel à un huissier pour faire constater le contenu de messages personnels de ses employés.
- *« Le respect de la vie personnelle du salarié ne constitue pas en lui-même un obstacle à l'application de l'article 145 du NCPC dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicités »*

Le contrôle de l'usage de la messagerie

RECOMMANDATIONS DE LA CNIL

- Admettre un usage raisonnable et ponctuel de la messagerie à des fins privées à condition de ne pas affecter le trafic normal des messages professionnels
- Mettre en place des outils de mesure de la fréquence et de la taille des fichiers transmis fréquence en pièce jointe ou des outils d'archivage des messages échangés
- En cas de mise en place de dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, déclaration à la CNIL

Le contrôle de l'usage de la messagerie

RECOMMANDATIONS

- Ne pas accéder directement au contenu des messages identifiés comme personnels :
 - sauf en présence du salarié concerné
 - sauf risque ou évènement particulier justifiant l'accès hors la présence du salarié

- Recourir aux mesures prévues par l'article 145 du NCPC pour préserver les preuves :
 - ordonnance du juge
 - accès au contenu par l'huissier
 - si possible en présence du salarié

L'utilisation de l'Internet

- **Utilisation abusive : licenciement pour motif personnel**

- **Conditions :**
 - ◆ utilisation des moyens informatiques mis à sa disposition
 - ◆ pendant le temps de travail
 - ◆ à des fins étrangères à l'activité de l'entreprise
 - ◆ utilisation d'une certaine gravité

- **Exigence d'une interdiction préalable de l'employeur ?**

L'utilisation de l'Internet

- **Preuve de la faute par des moyens informatiques**
 - ◆ Imputabilité de la faute au salarié
 - ◆ Heure, date et fréquence des utilisations
 - ◆ Collecte et conservation des preuves
 - ◆ Utilisation d'une certaine gravité

Le contrôle de l'utilisation de l'Internet

RECOMMANDATIONS DE LA CNIL

- Autoriser un usage raisonnable et ponctuel de l'Internet dans les conditions fixées par l'employeur
- Mettre en place des dispositifs de filtrage de sites non autorisés
- Interdire certaines pratiques illicites (téléchargement de vidéos ou de logiciels) ou susceptible de nuire aux intérêts de l'entreprise (chat, forums)
- Contrôler a posteriori et de manière non individualisée les données de connexion
- Déclarer à la CNIL si dispositif de contrôle individuel des durées de connexion ou des sites visités
- Elaborer des chartes d'utilisation assimilées au règlement intérieur de l'entreprise

Le recours aux chartes d'utilisation

- Objectifs de la charte
- Valeur juridique de la charte
- Forme et formalités

Les principes à respecter

- **Proportionnalité aux objectifs poursuivis (Art.120-2 du Code du Travail)**
- **Information préalable des salariés (Art.121- 8 du C.T.)**
- **Consultation des représentants du personnel (Art.432-2-1 et 2 et du C.T.)**
- **Déclaration à la CNIL (Loi Informatique et Libertés)**