# La charte informatique face aux nouveaux usages en entreprise

GS Days 2014

**Frédéric Connes**
Frederic.Connes@hsc.fr

**Amélie Paget**
Amelie.Paget@hsc.fr

# Plan

- Importance de la charte informatique
- **Nouveaux usages**
  - Multiplication des outils et services personnels en entreprise
  - Nouveaux outils et services d'entreprise
  - Nouveaux outils pour surveiller et échapper à la surveillance
  - Développement de la mobilité
  - Évolution des outils de communication

# Importance de la charte informatique

- S'est imposée comme un outil indispensable
- 3 axes
  - **Sensibilisation**
    - En complément des sessions de formation et des autres documents de gouvernance de l'entreprise
    - Notamment sur l'aspect sécurité (souvent demandée dans les audits ISO 27001)
  - **Information**
    - Informations concernant personnellement les salariés ***(art. L.1222-4 CT)***
    - Informatique et libertés ***(art. 32 LIL)***
  - **Sanctions disciplinaires**
    - Pour des faits analogues
      - Absence de charte et pas d'usage abusif : licenciement injustifié
      - Existence d'une charte : licenciement justifié

# Importance de la charte informatique

- **Opposable**
  - 3 possibilités
    - Signature par les utilisateurs
    - Annexion au contrat de travail
    - Annexion au règlement intérieur
      - Processus long et formel, mais recommandé
- **Actualisée**
  - Doit suivre les évolutions
    - Juridiques (normes, jurisprudences…)
    - Technologiques
    - Sociétales

  ⇒ Sa rédaction doit permettre une certaine pérennité
    - Renvois à des documents plus évolutifs
- **Sur mesure**
  - Adaptée au contexte de l'entreprise

# Multiplication des outils et services personnels en entreprise

« *Bring your own device* » (BYOD)

- **Définition**

  Matériel personnel utilisé dans le cadre professionnel

  → Ordinateur, tablette, ordiphone, objet connecté, clé USB, etc.

- **Risques**
  - Propagation de logiciels malfaisants depuis un matériel personnel mal sécurisé
  - Absence de contrôle de la sécurité des données stockées sur le matériel personnel
  - Fuite de données par l'intermédiaire du matériel personnel
  - Collecte d'informations confidentielles par le matériel personnel

    → Lunettes connectées, montres connectées, dictaphones…

# Multiplication des outils et services personnels en entreprise

- **A prévoir dans la charte informatique**
  - Interdire
  - Autoriser & Encadrer

A défaut, l'usage de matériels personnels est possible dans le respect du contrat de travail et du règlement intérieur

- Si autorisé, les données sont présumées professionnelles dès lors qu'elles sont accessibles depuis le SI de l'organisme
  - *Cass. Soc. 23 mai 2012*
    - Dictaphone non connecté : conditions d'accès à la sphère privée
  - *Cass. Soc. 12 février 2013*
    - Clé USB connectée : accès sans conditions (données professionnelles)

# Multiplication des outils et services personnels en entreprise

En cas d'autorisation

- **Autorisation préalable** par un responsable désigné
- Avec **acceptation des règles** imposées par l'entreprise
  - Application des mesures de sécurité
    - Signaler tout vol ou perte
    - Verrouiller l'outil, etc.
  - Acceptation d'un contrôle de l'appareil à tout moment
  - Restriction sur les données stockées/collectées sur le terminal
    - Ex. : accès distant sans copie locale
    - Rappel des infractions pénales
  - Retrait de l'autorisation à tout moment
    - Obligation d'effacer les données professionnelles et d'en justifier
- Encadrement des **sauvegardes** (personnelles/professionnelles)
- Rappeler les modalités d'**accès aux données par l'employeur**
  - Prise en main à distance
- Recommandation : **création d'un espace professionnel** sur les terminaux

# Multiplication des outils et services personnels en entreprise

« *Choose you own device* » (CYOD)

- **Définition**

  Achat par le salarié (avec possibilité de subvention de l'entreprise) sur un catalogue sélectionné par l'entreprise

- **Avantage** : maîtrise des matériels utilisés
  - Etude préalable des capacités en termes de sécurité
  - Installation d'outils de prise en main à distance, gestion des mises à jour, etc.
  - Configuration préalable commune déployée sur les matériels
  - Création d'un espace professionnel sur le terminal
- Seuls les matériels obtenus dans le cadre de cette procédure sont autorisés, au titre du BYOD
- Principe d'interdiction de modifier la configuration déployée

# Multiplication des outils et services personnels en entreprise

« *Bring your own software/service* » (BYOS)

- **Définition**
  - Logiciels personnels installés sur le matériel professionnel

  → Condition préalable : quand le salarié dispose des droits suffisants
  - Services personnels accessibles par un logiciel ou un navigateur depuis le poste professionnel

  → Navigateur : ne nécessite pas de droits particuliers
- Données **présumées professionnelles**
- **Risques**
  - Installation de logiciels malfaisants
  - Installation de logiciels illicites ou sans licence
  - Fuite de données (accidentelle ou non)
  - Non-conformité

  → Non conformes aux politiques de l'entreprise

  → Problème d'interopérabilité

# Multiplication des outils et services personnels en entreprise

A encadrer dans la charte

- Interdiction
- Autorisation sous conditions
  - En fonction du logiciel ou du service dont l'utilisation est demandée
  - Logiciels : démontrer le respect de la licence
  - Ne pas utiliser à des fins professionnelles
  - Si utilisation à des fins professionnelles
    - Demande démontrant pourquoi le besoin n'est pas satisfait par les outils déjà à disposition
    - Etude des risques, notamment de fuite de données, par le demandeur
    - Accord écrit de la direction, retirable à tout instant
    - Contrôles périodiques de l'utilisation du logiciel ou du service

# Nouveaux outils et services d'entreprise

« *Corporate Owned Personally Enabled* » (COPE)

- **Définition**

  Matériels, logiciels, services fournis par l'entreprise pour travailler, avec un usage personnel toléré

  Le salarié peut choisir son matériel et les logiciels professionnels sur un catalogue proposé par l'entreprise

- Alternative au BYOD/BYOS
- Données **présumées professionnelles**

⇒ Dans la charte

- Imposer l'usage exclusif des matériels, logiciels et services fournis par l'entreprise
- Autoriser l'usage personnel
  - Au temps de travail, usage raisonnable
  - Dans un contexte privé, sous réserve du respect de la politique de sécurité et des obligations de loyauté et de confidentialité

# Nouveaux outils et services d'entreprise

« *Cloud computing* »

- Nombreux risques pour la sécurité
  - → Disponibilité, intégrité, confidentialité, auditabilité, maîtrisabilité

**A encadrer dans la charte**

- Interdire ou autoriser l'usage d'espaces *cloud* personnels
- Interdiction ou autorisation d'accès au service depuis l'extérieur du SI de l'entreprise
- Définir un périmètre
  - Selon la criticité des données
    - Chiffrement obligatoire pour certains types de données
    - Fonctionnalités interdites à certains niveaux de classification
  - Selon les services concernés
- Interdiction d'utiliser en parallèle un compte professionnel et un compte personnel sur le même service
- Interdiction d'interfacer ou de synchroniser le service avec un autre service, personnel ou professionnel

# Nouveaux outils et services d'entreprise

**Biométrie** sur les terminaux professionnels

- Multiplication des offres
- Ordinateurs, tablettes, ordiphones…
- Souvent par empreinte digitale

Exigences « informatique et libertés »

- Possible pour le **contrôle d'accès** au terminal
  - Interdiction de principe du contrôle des horaires
- **Autorisation** de la CNIL
  - Plusieurs autorisations uniques ***(n°AU-027)***
- **Difficultés**
  - Élément personnel confié à un dispositif professionnel
  - Ne peut pas être modifié (identification plus qu'authentification)
  - **Difficile à imposer**
    - Recommandé de permettre des alternatives (mot de passe fort)

⇒ Information dans la charte

# Nouveaux outils et services d'entreprise

**Géolocalisation** des terminaux mobiles professionnels

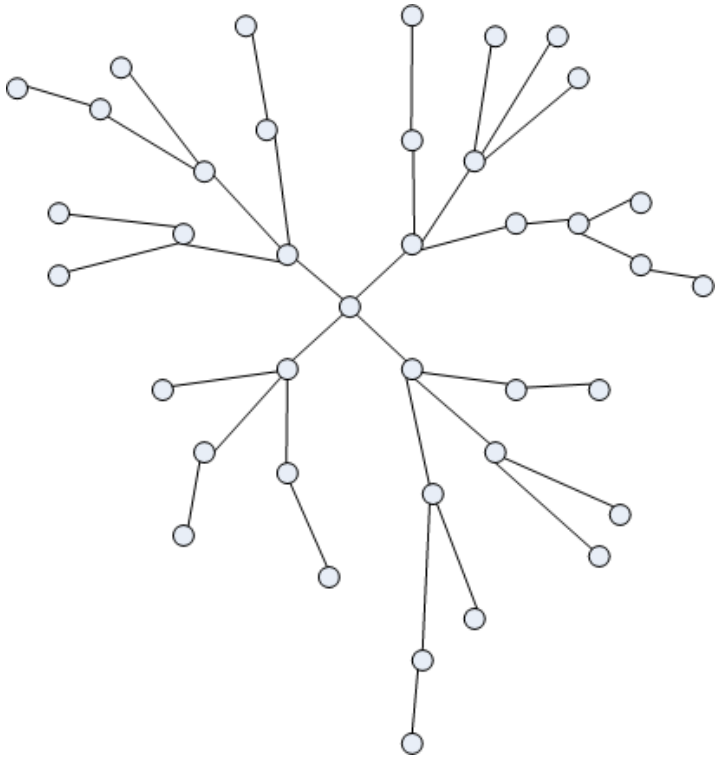
- Fonctionnalité offerte par certains fabricants et éditeurs
- Difficulté : peut permettre une surveillance permanente des salariés à distance
- Conformité à la loi « informatique et libertés »
  - Déclaration à la CNIL
  - Principe d'exclusion du contrôle de l'activité des salariés comme finalité

⇒ Dans la charte

- Indiquer les finalités de l'outil
- Fonctionnalité désactivée en dehors des heures de déplacement
- Imposer l'activation à certaines heures
- Possibilité d'activation à distance dans certains cas (de perte, vol, ou urgence médicale, etc.)

# Nouveaux outils pour surveiller et échapper à la surveillance

## Données relatives au trafic



- ***Art. L.34-1 CPCE***
  - Conservation des données de trafic
  - Pas de conservation des contenus
  - Applicable aux connexions des salariés ?
- Surveillance de l'activité des salariés
  - Données présumées professionnelles
  - Information des salariés, par exemple dans la charte informatique
  - Possibilité de prévoir des plages de liberté de connexion
- Filtrage des connexions
  - Possible, à mentionner dans la charte informatique

# Nouveaux outils pour surveiller et échapper à la surveillance

Interception SSL « *man in the middle* »

- **Définition**

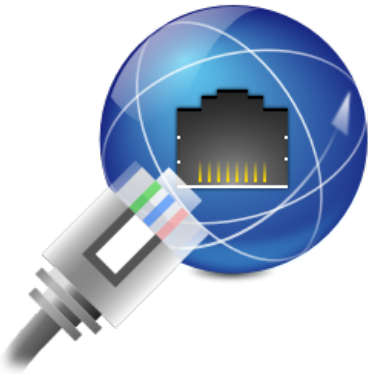
  *Proxy* qui déchiffre puis « rechiffre » les flux chiffrés (HTTPS)

  ⇒Passage temporairement en clair du trafic que le salarié pensait être chiffré, donc potentiellement confidentiel

  - Banque, commerce en ligne, factures, santé, etc.
- Nécessite toujours une action sur le poste du salarié
  - Installation du certificat du *proxy* de l'entreprise
  - Mais peut être préinstallé sur le poste fourni, et donc ignoré de l'utilisateur
- Même encadrement qu'avec un *proxy* « classique »
- Mais **informer spécifiquement** dans la charte informatique
  - Mise en place d'outils de déchiffrement SSL
  - Surveillance et filtrage possibles sur le trafic chiffré

# Nouveaux outils pour surveiller et échapper à la surveillance

« *Bring your own connection* » (BYOC)



- **Définition**
  - Installation d'un accès Internet personnel en entreprise
  - Utilisation du partage de connexion d'un ordiphone
    → Invisible physiquement
  - Permet d'échapper à la surveillance de l'employeur et au filtrage
  - Générateur de risques pour la sécurité du SI
- Visible par l'employeur

  → Connexions entrantes au système d'information depuis l'extérieur alors que le salarié est dans l'entreprise

- Peut être interdit par la charte informatique
  - Si pas explicitement interdit, c'est autorisé
  - Rester cohérent avec les règles du travail à distance

# Nouveaux outils pour surveiller et échapper à la surveillance

**Tunnels** montés par les salariés à partir de l'entreprise vers une machine non-professionnelle

- Service spécialisé ou serveur dédié personnel
- Souvent par des salariés disposant de compétences techniques

- Permet de masquer l'ensemble du trafic sortant
  - Et donc d'échapper à la surveillance et au filtrage
- Identifiable par l'employeur
- Conséquences :
  - Perte de contrôle de l'employeur sur l'usage de l'outil professionnel
  - Risque pour la sécurité du système d'information
  - Aucun intérêt professionnel car l'employeur offre déjà une connexion à Internet

⇒ Peut être interdit par la charte informatique

# Développement de la mobilité

- Nouveaux outils de nomadisme facilitant
  - Travail à domicile
  - Travail en déplacement
  - Connexion permanente au SI de l'entreprise
- Depuis un outil professionnel ou personnel
- **L'encadrement de la mobilité est essentiel**
  - Charte informatique peut restreindre la mobilité à l'utilisation d'un appareil professionnel
  - Appareil personnel : dans le cadre fixé pour le BYOD ou du *cloud computing*
  - Doit s'accompagner d'une politique de gestion des terminaux mobiles

# Développement de la mobilité

Dans la charte

- Rappeler l'obligation de sécurité
- **Encadrer les connexions**
  - Interdiction des connexions sur les *wifi* publics, les réseaux filaires non fiables, etc.
  - Obligation de connexion au SI en VPN, en excluant toute connexion simultanée à Internet via la connexion locale
- **Chiffrement** de l'outil ou de l'espace de stockage des données professionnelles
- **Verrouillage** systématique du poste, même chez soi
- Règles de **mot de passe** spécifiques sur les terminaux
  - Respect de la politique de mot de passe de l'entreprise (mot de passe fort)

# Développement de la mobilité

- Précautions à prendre dans les **lieux publics**
  - Rappel sur les risques d'espionnage
  - Train, avion, conférence, etc.
  - Obligation d'utilisation d'un filtre écran
  - Interdiction d'utilisation d'un téléphone mobile non verrouillé dans un environnement présentant des risques de vol
- **Ne jamais laisser l'appareil sans surveillance**, sauf dans un lieu privé
  - Domicile, chambre d'hôtel, etc.
  - Toujours éteint (pas en veille)

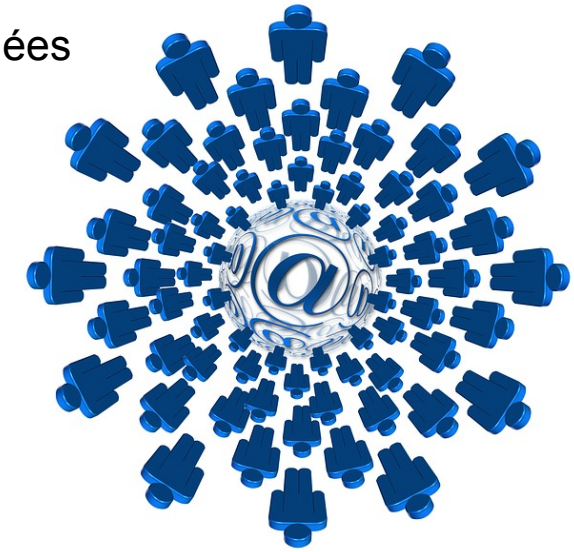
# Développement de la mobilité

- Déplacements dans un **contexte « à risque »**
  - Respecter la législation locale des États étrangers
    - Problématique des outils de chiffrement
  - Ne stocker aucune donnée sur le disque
    - Accès exclusivement par le réseau
- **Retrait des droits d'accès à distance** à certaines conditions
  - Non-respect constaté des obligations de sécurité
  - Congés, arrêts, etc.
- Problématique des **horaires de travail**
  - Suspension de l'accès en dehors du temps de travail
    - Gestion des fuseaux horaires à intégrer en cas de déplacements professionnels

# Évolution des outils de communication

Différents médias

- Réseaux sociaux, forums, espaces de contribution, messageries instantanées
- Externes ou internes à l'entreprise
- A tendance professionnelle ou personnelle



## Médias externes

- Au temps de travail : généralités
  - Interdiction
  - Autorisation
    - Condition d'un usage raisonnable
    - Rappel de la responsabilité des salariés, de leur obligation de loyauté et de confidentialité
      - Même en cas de publications réalisées en dehors du temps de travail
  - Possibilité de filtrage
  - Accès de l'employeur
    - Échanges publics : pas de difficulté
    - Échanges privés : régime du secret des correspondances

# Évolution des outils de communication

→ Traitement différents pour les publications portant sur des **sujets professionnels**?

→ Publications majoritairement publiques

- **Publication en leur nom**
  - Certains organismes souhaitent les encourager
  - Plus tolérante sur le temps passé sur ces réseaux aux heures de travail
  - Rappel de l'obligation de loyauté et de confidentialité et de la responsabilité du salarié
- **Publications réalisées au nom de l'entreprise**
  - Dans quel cadre le salarié est-il considéré comme s'exprimant au nom de l'entreprise ?
    - Référence à sa qualité de salarié dans le contenu, signature, etc.
  - Autorisation générale pour certains (*community managers*, directeurs…)
  - Autorisation préalable écrite de la direction pour les autres
  - Autorisation circonscrite à certaines publications spécifiques
  - Susceptible d'engager la responsabilité de l'entreprise

# Évolution des outils de communication

## Médias internes

→ Quelles sont les limites de la liberté d'expression des salariés ?

- Sentiment de liberté sur les contenus publiés
  - *« On est entre nous »*

⇒ Possibilité de **rappeler les bons usages** dans la charte

- Caractère professionnel des médias
- Obligation de loyauté envers l'employeur
- Respect des collègues
- Respect des clauses de confidentialité à l'égard des autres collègues
- Interdiction des échanges de contenus illicites
- Interdiction des dérives non professionnelles
- Ne pas nuire au bon fonctionnement du SI

- **Accès de l'employeur** à l'ensemble des échanges

  → Autoriser ou pas la création de canaux d'échange privés

# Conclusion

- Multiplication des nouveaux usages en entreprise
  - Avec l'apparition de nouveaux outils
  - Tant par l'entreprise que par les salariés
  - Nécessitant parfois des compétences techniques
- Interconnexion croissante entre les sphères personnelle et professionnelle
- Augmentation des risques pour la sécurité du système d'information de l'entreprise

⇒ Ces nouveaux usages sont progressivement pris en compte au sein des chartes informatiques

# Références


- Alexis Contamine, « La surveillance des salariés », Colloque, 28 mai 2013, Les programmes de conformité – enquêtes internes de concurrence, *Lamy de la Concurrence*, 2013, n°37
- « Règlement intérieur et autres normes patronales d'entreprise », Fascicule 1-40, *Jurisclasseur Travail Traité*, LexisNexis, cote 04,2010
- Legifrance : http://www.legifrance.gouv.fr/
- Code du travail
- Code des postes et des communications électroniques
- Code pénal, Code civil
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi du 6 août 2004

# Références


- Soc., 14 janvier 2014, *sté Transports Goubet,* 12-16.218
- Soc., 18 décembre 2013, *Rem c. M. X.,* 12-17.832
- CA Orléans, 16 mai 2013
- CA Lyon , 13 mars 2013
- CA Versailles 22 février 2012
- Soc., 26 janvier 2012, 11-10.189
- CA Rouen, 15 novembre 2011, *Mylène E. c. Vaubadis*
- Soc., 15 décembre 2010, *Emmanuel G / Coca Cola*, 09-42.691
- CPH Boulogne-Billancourt, 19 novembre 2010
- CA Dijon, 14 sept. 2010
- Soc., 8 décembre 2009, *Sergio G. / Peugeot Citröen*, 08-42.097
- *Arrêt BNP Paribas*, CA Paris, 4 février 2005
- *Arrêt Nikon*, Soc., 2 octobre 2001, 99-42.942
- Soc., 13 novembre 1996, 94-13187

# Questions