

# Aspects légaux de l'informatique

Pierre-Yves Bonnetain-Nesterenko  
py.bonnetain@ba-consultants.fr

ENSEEIH 3A – TLS-Sec  
B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

Octobre-novembre 2019



- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code. . .
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingénierie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR ([www.ossir.org/resist](http://www.ossir.org/resist))

Un certain nombre de textes prennent en compte :

- Les atteintes au fonctionnement des systèmes informatiques (au sens large).
- Les atteintes à la vie privée, potentielles ou avérées.
- La protection de la correspondance privée.
- Et plein d'autres choses sympathiques.

Cela va sans dire

La loi française s'applique en France uniquement.

Internet n'est pas une zone de non droit

Un délit/crime informatique matérialisé en France peut être poursuivi en France, même si les serveurs sont à l'étranger.

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# Lois pénales directement applicables

Deux grands textes, transcrits dans le Code Pénal, sont directement applicables à l'informatique :

**Article 226-16 et suivants** Ex-loi Informatique et Libertés. Concerne les traitements automatisés de données nominatives.

**Article 323-1 et suivants** Ex-loi Godfrain. Concerne toutes les atteintes au fonctionnement des systèmes de traitement de données.

## Règlement Général pour la Protection des Données

RGPD applicable depuis 28 mai 2018. Change énormément de choses sur les données personnelles.

# Usage de ces deux textes

- ~~Art. 226-16 et suivants : vos données nominatives sont « mal protégées » par un tiers, une collecte paraît illégitime, ...~~
- Art. 323-1 et suivants : vous êtes victime d'une attaque (intrusion, déni de service, vol de données, ...)

## Note à l'usage des gens normaux

Il est parfois « quelque peu difficile » de faire enregistrer sa plainte par les forces de police ⇒ pour une entreprise, cela doit se préparer en amont (qui contacter ?).

## Attention

L'entreprise qui se fait voler ses données ~~peut être accusée (au sens du 226-16) par ses clients (protections inadéquates)~~ va sérieusement en baver.

# Concernant les données à caractère personnel

Il est nécessaire de bien comprendre que :

- Le responsable du traitement a une **obligation de moyens**.
- Les moyens mis en œuvre doivent correspondre à la criticité des données.
- Le responsable du traitement est considéré comme **connaissant la sensibilité des données** qu'il gère ou fait gérer.
- Le responsable du traitement reste **responsable même en cas de sous-traitance** des traitements (cf CNIL/Darty).
- RGPD : les sous-traitants sont co-responsables

## Conclusion évidente

Si vous pouvez, évitez de traiter des données nominatives, ou minimisez celles que vous traitez. . . C'est plus facile qu'on ne le croit.



# Qu'est-ce qu'une DCP

## Donnée à caractère personnel

Toute donnée ou information dont le contenu permet, de façon directe ou indirecte, d'identifier son porteur ou propriétaire

Donc, potentiellement, beaucoup de choses. Y compris si forme non numérique. ~~**Conclusion** Il est conseillé de toujours déclarer ses traitements à la CNIL. Déclaration supprimée avec RGPD.~~

## Conclusion

*Da Scritch, Capitole du Libre 2017* : Une DCP, c'est comme de la matière fissile. Si tu ne sais pas la collecter, la stocker et la détruire, surtout tu n'y touches pas.

# Pour faire simple

Une donnée à caractère personnel, c'est

Toute brève d'information permettant d'identifier une personne.

Exemples :

- photos ou vidéos,
- adresses électroniques, numéros de téléphone,
- e-mails, messages vocaux. . .

## Attention

Ne confondez pas **données personnelles** avec **données privées**. Les secondes sont **incluses** dans les premières, mais n'y sont pas égales.

# Et autour des données ?

Méta-données peuvent aussi être (très) identifiantes :

- listes d'appels téléphoniques ou SMS envoyés (qui communique avec qui, quand, à quelle fréquence, quelle durée. . . )
- méta-informations ajoutées dans des fichiers (images, vidéos, bureautique. . . )
- recherches réalisées sur un moteur de recherche, traces de navigation sur le web, résolutions DNS
- traces GPS, traces de migration d'antennes mobiles.

# Vie privée, vie personnelle et données

Chacun devrait toujours se poser quelques questions :

- Où sont mes données nominatives et mes données privées ?
- Qui en est responsable ?
- Qui y a accès ?
- Quelles sont les règles d'engagement de ces données ?
- Qu'arrivera-t-il, que m'arrivera-t-il si ces données deviennent publiques, volontairement ou à mon insu ?

## Garder à l'esprit

Ces questions, et les réponses inappropriées qui peuvent y être apportées par les entreprises, sont autant de risques personnels (propriétaire légitime) et opérationnels et juridiques (entreprise responsable).

# Du point de vue de l'entreprise

Inverser les questions précédentes.

**Dès lors** qu'il y a collecte d'informations nominatives. . .

- 1 Comment y donner accès pour leur propriétaire (droit d'accès et de rectification, obligation CNIL) ?
- 2 Pour quelle utilisation les propriétaires ont-ils confié ces données ? Ne fait-on bien que ces traitements et aucun autre ?
- 3 Où et comment sont-elles stockées, archivées, sauvegardées ?
- 4 Qui en a la responsabilité technique ? opérationnelle ?
- 5 Qui peut y avoir accès au sens opérationnel et au sens technique ?

*Liste poursuivie sur transparent suivant*

# Du point de vue de l'entreprise – suite

**Dès lors** qu'il y a collecte d'informations nominatives...

- ⑥ Dans quelles situations ces données peuvent-elles être utilisées ? Transmises à des tiers ? Vendues ? Est-ce bien dans les règles de collecte initiales ?
- ⑦ Quelles sont les règles de conservation et d'effacement de ces données ? Comment sont-elles appliquées ?
- ⑧ Quelles sont les conséquences pour nous/nos clients en cas de perte/fuite de ces données ?

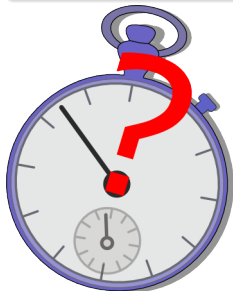
## Bien trop souvent

Aucune de ces questions ne reçoit de réponse vraiment pertinente la première fois qu'on les pose. RGPD : registre des traitements et EIVP obligent à se poser ces questions.

# Petit exercice

Ce n'est pas si difficile qu'on le pense...

Comment peut-on (espérer) détecter que l'entreprise s'est fait voler des données (particulièrement des données nominatives de clients) ?



Ca peut facilement arriver :

- Collaborateur parti à la concurrence avec des fichiers de l'entreprise
- Incident de sécurité et vol de données
- Matériel « jeté » sans avoir été nettoyé auparavant
- etc.

# CNIL, RGPD, données personnelles et entreprises

N'oubliez pas l'imbrication :

- 1 La loi « Informatique et libertés » et le RGPD donnent des **droits** aux propriétaires des données nominatives, c'est-à-dire aux particuliers.
- 2 Ces droits imposent des **devoirs** aux entreprises responsables de traitements de données nominatives.
- 3 Ces devoirs vont devenir des contraintes **très** fortes.

## Le sens de l'histoire

Le respect de ces devoirs va devenir de plus en plus contrôlé (cf RGPD)



# Ça commence à taper

- Pré-applicabilité RGPD
  - Janvier 2018, Darty amende 100 000 €
  - Janvier 2018, PhoneWarehouse UK amende 500 000 €
  - Juin 2018, Optical Center, 250 000 €
  - Juin 2018, Association pour le Développement des Foyers, 75 000 €
  - Juillet 2018, OPH Rennes, 30 000 €
  - Août 2018, DailyMotion, 50 000 €
- Post-RGPD
  - Septembre 2018, Alliance Francaise Paris Ile De France 30 000 €
  - Janvier 2019, Google, 50 millions €
  - Juin 2019, Liga Espagnole, 250 000 € ; Sergic, 400 000 €
  - Juillet 2019, Mariott, 110 millions € ; British Airways 210 millions €

# Une nouveauté qui a bien évolué

## Telcos' data breach notification amendment is passed

OUT-LAW News, 03/11/2009

The European Council has approved a data breach notification rule for Europe's telecoms firms. The amendment to an EU Directive will force telcos to tell customers if they lose their data.

The European Parliament and Commission have already approved the amendments, which will become law after it has been published in the EU's Official Journal and signed by the President of the Council and President of the European Parliament.

The amendments, though, do not extend data breach notification duties to non-telecoms firms, despite the Parliament's earlier demands that it include providers of 'information society services' such as online banks or health services providers.

- 2009 – Discussions pour obligation étendue à toute entreprise gérant des données nominatives – projet Escoffier-Détraigne
- 2011 – Ordonnance n° 2011-1012 (24 août) relative aux communications électroniques

Depuis 25 mai 2018

RGPD, obligation de notification

## Conséquences

- Etre capable de détecter l'incident (quelles données perdues ?)
- Etre en mesure d'identifier sa portée (qui est touché ?)

# Une évidence à rappeler

## Une information que vous n'avez pas ne fait courir aucun risque à personne.

- RGPD **impose** minimisation des données (volume et durée)
- Nécessité analyse fine processus consommation des données
- Anonymisation ou pseudonymisation
- Études d'impacts sur la vie privée

# Conséquences

## Développeurs, architectes, exploitants. . .

Il faut partir sur des bases saines de conception (obligatoire depuis RGPD)

- orientée confidentialité (privacy by design)
- et orientée sécurité (security by design)

## Commerciaux, responsables clients, marketing. . .

Intégrer dans vos réflexions et projets

- l'opportunité de collecter certaines informations
- les contraintes liées aux données qui sont collectées
- les procédures d'effacement des données
- les risques et conséquences du moindre incident.

Tout cela **AVANT** la mise en production.

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - **Lcen, Loppsi2**
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# LCEN – 21 juin 2004

- Loi pour la Confiance dans l'Économie Numérique
- Transcription directive européenne 2000/31/CE
- Traçabilité des usages
  - Hébergeur contenus : adresse IP, identifiant interne, protocole utilisé, opération (création, modification, suppression), date et heure
  - FAI : IP fournie, identifiant interne, MAC si dispo, dates et heures début/fin cnx, caractéristiques ligne (Wifi, ADSL, 3/4G...)
- Durée conservation 12 mois (retoquée CJUE décembre 2016)

- Obligations hébergeurs contenus
  - responsabilité a posteriori sur notification contenus illégaux ou protégés
  - encadrement précis des notifications (fond et forme)
  - notification non justifiée : 1 an, 15 000 €
- Article 323-3 CPP : introduction infraction d'intrusion dans un STAD
- Commerce/communication électronique : mentions légales sur site
- Consentement (opt-in) pour traitements données nominatives

# LCEN – mentions légales

- Site personnel
  - coordonnée hébergeur (sur requête judiciaire, doit pouvoir fournir coordonnées client)
- Site professionnel
  - nom et adresse société, capital social
  - SIRET
  - nom et coordonnées directeur publication
  - coordonnées hébergeur



# LOPSSI 2 – 14 mars 2011

- Loi d'Orientation et Programmation pour la Performance de la Sécurité Intérieure
- Introduit blocage administratif de sites
  - listes noires (non publique) de sites
  - listes noires (non publique) d'adresses IP
  - autorisation (sous contrôle juge) intrusion dans système informatique

## Notez bien

Trivial contourner listes noires sites/IP

Tous FAI n'ont pas les listes de blocage

Possible d'être en liste noire par abus/dérapage/erreur

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - **Pourquoi le RGPD**
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# Nous revenons de loin

Entre 2007 et 2011...

- Changements réguliers politique de vie privée de Facebook, fiasco dénoncé « the next Facebook privacy scandal »
- Eric Schmidt (PDG Google, 2009) : « Only miscreants worry about privacy » et « If you don't want it known, don't do it »
- 22 infractions majeures de Facebook à la législation irlandaise sur la protection des données personnelles (2011)
- Directive européenne et 28 pays → 28 lois avec variations

## Conséquences

Nécessité de changement significatif de la législation en place pour apparition « véritables sanctions » et « une même règle pour tous »

# Cibles principales

- Pas forcément les GAFA
  - bien meilleure gestion des risques juridiques
  - certaines déjà condamnées sous régime actuel (3 M € max)
  - nette avance protection données personnelles
- plutôt les entreprises européennes
  - faible culture gestion risques juridiques
  - ne comprennent pas besoin protection données personnelles
  - peu de compétences en la matière

# Principales évolutions

- règlement et non directive européenne
- homogénéisation probable (décisions, sanctions) niveau européen
- sanctions dissuasives (2 à 4% CA mondial, 10/20 M € pour administrations, arrêt traitement)
- conservation majorité obligations antérieures
- suppression déclaration CNIL au profit responsabilisation et autocontrôle
- nouvelles obligations de sécurité
- étude d'impact obligatoire, avant mise en œuvre, pour certains traitements (données sensibles, profilage)
- renforcement droits personnes notamment sur preuve consentement

# Et aussi...

- co-responsabilité **automatique** sous-traitants (y compris GAFAM...) → contractualisation impérative
- obligations « sécurité et confidentialité par conception » (pour les données nominatives)
- portabilité données personnelles
- obligation notification violations

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# Registre des traitements – 1

- Tracer tous traitements de données personnelles
- Théoriquement selon taille entreprise ( $\geq 250$  personnes)
- Obligatoire prouver conformité tous traitements
- Difficile sans liste exhaustive
- Registre doit être tenu à jour

## Informatique interne

- ◇ Accès salles informatiques
- ◇ Traçabilité actions
- ◇ Gestion sauvegardes
- ◇ Outils prise contrôle à distance
- ◇ Gestion activité administrateurs
- ◇ Suivi outils bureautique
- ◇ Suivi photocopies/impressions
- ◇ Paie, congés, gestion RH
- ◇ Applications installées sur postes

## Intranet

- ◇ Annuaire (LDAP/AD)
- ◇ Organigramme
- ◇ Site intranet
- ◇ Enquêtes satisfaction internes
- ◇ Système surveillance/sécurité
- ◇ Journaux activité
- ◇ Vidéosurveillance
- ◇ Messagerie

## Internet

- ◇ Site web
- ◇ Lettre d'information
- ◇ Espace emploi
- ◇ Réseaux sociaux
- ◇ Fora discussion

## Évolution poste

Désigner un délégué à la protection des données (*data privacy officer*).  
Obligatoire dans secteur public, ou si traitements à grande échelle



# Registre traitements – 2

Registre doit indiquer, pour chaque traitement

- nom et coordonnées responsable(s) traitement et délégué à la protection des données
- finalités traitement
- catégories personnes concernées et catégories données personnelles
- catégories destinataires données, y compris tiers, hors pays collecte ou entité internationale
- existence transferts hors pays collecte ou vers entité internationale
- délais effacement selon catégories des données (quand donnée devient-elle inutile?)
- description générales mesures de sécurité techniques et organisationnelles

# Minimisation des données

- Uniquement données personnelles *strictement nécessaires* pour chaque traitement
- Purger/nettoyer données existantes (volume collecté et durée conservation)
- Réflexion de fond sur *tous* traitements existants
- Avec contraintes légales de conservation de certaines données

## Exemple minimisation

Liste de diffusion : adresse électronique (et rien d'autre)

Départ collaborateur : garder informations légales (contrat, versements, etc.), éliminer l'inutile (dates congés pris, photo pour badges, etc.).

# Licéité traitement et consentement

Traitement licite si au moins une condition remplie :

- 1 Consentement explicite, éclairé et univoque
- 2 Traitement nécessaire pour exécution contrat (ou mesures précontractuelles) auquel la personne est partie
- 3 Traitement nécessaire pour respect obligations réglementaires du responsable du traitement
- 4 Traitement nécessaire pour sauvegarde intérêts vitaux personne ou tiers
- 5 Traitement nécessaire pour exécution service intérêt public par responsable du traitement

# Consentement

- Consentement explicite, éclairé et univoque
- Fournir toutes informations nécessaires pour prise décision
- Pouvoir apporter preuve consentement utilisateur

## Exemples

- lettre information : consentement explicite
- cafétéria : consentement explicite
- paye : obligation légale (noter celle-ci)

## Questions en suspens

Que faire pour traitements anciens, non conformes (pas trace consentement explicite) ?

Fournisseur peut-il dire « faute d'acceptation de tous ces traitements, pas de service » ?

# Mentions légales – 1

- identité et coordonnées responsable du traitement
- coordonnées *délégué à la protection des données* s'il existe
- finalité et base juridique traitement
- destinataires données
- transfert éventuel vers pays tiers/organisation internationale

# Mentions légales – 2

- durée ou critères conservation
- droit d'accès, de rectification, d'effacement
- droit de limitation ou d'opposition au traitement
- droit de retrait du consentement
- droit réclamation auprès autorité de contrôle
- indication si fourniture données est à caractère réglementaire, contractuel ou conditionne conclusion contrat
- informations sur données obligatoires ou non et conséquences non fourniture données

# Portabilité données

- Pouvoir fournir à l'intéressé *toutes les données* le concernant
- Dans délais raisonnables
- Dans format structuré, couramment utilisé, lisible par une machine

## Attention !

Impératif vérifier demandeur a pleine légitimité à faire la demande.  
Héritier/époux/maîtresse ne sont pas légitimes sans accord explicite du propriétaire (si décédé... compliqué).

# Obligation notification

- Dans les meilleurs délais, de préférence sous 72 heures après détection incident
- violation (accidentelle ou intentionnelle) sécurité avec perte, destruction, altération, divulgation ou accès non autorisé(s)
- notification CNIL (prioritaire) et personnes concernées (un peu moins, mais doivent être prévenues)
- notification doit indiquer
  - description nature violation, catégories et nombre victimes, volume données concernées
  - nom et coordonnées DPD
  - conséquences probables pour victimes
  - mesures remédiation ou atténuation mises en place
  - mesures pour prise en charge préjudice



# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# Quelques autres textes applicables

- Code de la Propriété Intellectuelle (contrefaçons), qui prévoit le cas des logiciels.
- Code Monétaire et Financier (moyens électroniques de paiement).
- DADVSI, Hadopi, Loppsi-1, Loppsi-2. . .

# Autres textes

Sont indirectement applicables :

- Loi de 1881 sur la presse (diffamation, incitation à la haine, apologie de crimes...).
- Lois et règlements sur le secret de la correspondance.
- Lois concernant la mise en péril de mineurs (notamment exposition à des contenus pornographiques).

Les plus intéressants sont les textes et décisions touchant au secret de la correspondance et au respect de la vie privée.

# Une jurisprudence mouvante

De nombreux points évoluent rapidement, dans des directions parfois contradictoires :

- En fonction du contexte
- En fonction des acteurs
- En fonction du libellé des plaintes

## Exemple

Protection de la vie privée vis-à-vis du contrôle du poste de travail par l'employeur.

## Bon à savoir

Ne jamais généraliser une décision de justice sans connaître le dossier.

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# La vie privée et l'entreprise

- Attente logique d'un respect de la vie privée des collaborateurs.
- **Tolérance** institutionnalisée (en France) d'un empiètement de la vie privée dans la vie professionnelle (appels privés, mails privés. . . )
- Tout est question de dosage et de contexte.
- L'entreprise **peut** surveiller, mais **doit** informer les représentants du personnel et ses collaborateurs.
- Les collaborateurs **doivent** loyauté à leur employeur.

Une fois cela dit

Tout est possible selon les situations.

# Tout est dans le contexte

**Legalis.net** propose sur son site l'intégralité de **l'arrêt** du 8 décembre 2009 qui a cassé les jugements précédents. La Cour de cassation, considérant que la Cour d'Appel n'a pas recherché "... comme elle y était pourtant invitée, dans quelle mesure cette utilisation personnelle de l'ordinateur professionnel avait nui à la bonne qualité de la prestation de travail de Monsieur X..." a dit que "...la seule conservation sur son poste informatique de trois fichiers contenant des photos à caractère pornographique sans caractère délictueux ne constituait pas, en l'absence de constatation d'un usage abusif affectant son travail, un manquement du salarié aux obligations résultant de son contrat susceptible de justifier son licenciement".

**Traduction :** "... un fait relevant de la vie privée peut être sanctionné si l'employeur prouve la répercussion sur l'exécution du contrat de travail. Le régime est donc extensif, mais il faut prouver". **Actualités du droit.**

Les **notes de service** et **chartes informatiques** pèsent le même poids que le règlement intérieur : significatif pour des mesures disciplinaires, insuffisant pour des sanctions fortes.

# Entreprise et vie privée

## Situation générale

L'ordinateur mis à disposition par l'entreprise est à but professionnel. **Tout ce qu'il contient est réputé professionnel**, sauf mention explicite contraire.

Pour simplifier un peu :

- L'employeur peut, **à volonté**, examiner le disque dur d'un poste de travail (ou la messagerie, etc.)
- Les zones ou éléments marqués comme privés peuvent être lus, mais **uniquement** après information du collaborateur



# Entreprise et vie privée

- En cas de suspicion, invoquer la protection de la vie privée ne permet pas d'empêcher l'accès aux données.
- Mais il faut **absolument** que ce soit encadré juridiquement pour l'employeur.

## Détail intéressant

Une clé USB personnelle **connectée** à un ordinateur professionnel **peut être examinée** par l'employeur (sauf mention explicite sur la clé comme quoi elle est personnelle).

## Et demain ?

Utilisation de plus en plus fréquente de matériel personnel (tablette, téléphone portable) pour travailler (BYOD)...

# Zones personnelles sur poste de travail

Il existe donc un **droit de regard volumétrique** des espaces personnels sur le poste professionnel, mais pas de **droit d'examen détaillé** en dehors de l'information/présence/accord du salarié.

## L'employeur peut

- Demander la suppression (tolérance zéro) de données classifiées comme personnelles,
- ou empêcher leur sauvegarde,
- voire les supprimer d'autorité.

## Par contre, il **ne peut pas**...

... lire le contenu de ces zones (sauf nécessité technique impérieuse) **sauf** en présence du salarié, qui peut se faire assister (procédure formelle de contrôle).

# Attention aux pièges de la vraie vie

- Responsable informatique licencié pour avoir consulté la messagerie du PDG, récupéré des documents sur les rémunérations et envoyé tout cela à son avocat
- Preuves collectées par l'entreprise en consultant la boîte à lettres du salarié, absent ce jour là.
- Prud'hommes et appel, licenciement justifié.
- Jugement cassé (26 juin 2012) car règlement intérieur interdit consultation des messages, y compris messages non-personnels, en l'absence du salarié.

## En résumé

Si le règlement intérieur donne des droits complémentaires au salarié, ceux-ci s'appliquent pleinement.

# Chiffrement sur poste de travail

Deux possibilités clairement disjointes :

- 1 Données personnelles chiffrées : contraintes liées aux données privées s'appliquent. Peut être demandé leur déchiffrement (dans le cadre des procédures appropriées), mais **pas** le mot de passe de déchiffrement.
- 2 Données professionnelles chiffrées : l'entreprise **peut exiger** de disposer du mot de passe de déchiffrement (pas toujours malin, mais... ) ou mettre en place des méthodes d'accès supplémentaires.

## Posez-vous la question

Le chiffrement de données professionnelles sur le poste de travail signifie que le collaborateur **ne veut pas** que ses collègues voient ces données. . .  
Il ne s'agit pas d'une protection contre le vol de l'ordinateur.

# Plan

- 1 Principaux textes de lois
  - I&L, Godfrain
  - Lcen, Loppsi2
  - Pourquoi le RGPD
  - Principales conséquences
- 2 Autres textes
- 3 Vie privée, Internet, jurisprudence et autres
- 4 Surveillance des activités

# La surveillance des activités

La surveillance est un élément légitime et nécessaire dans toute entreprise. Toutefois,

- Le contenu des informations collectées, le but de la surveillance, les modalités d'accès aux informations doivent être clairs.
- Surveiller n'est pas intercepter (art. 432-9 CP).
- La durée d'archivage et les procédures de destruction doivent être définies.

Et surtout . . .

La surveillance ne peut se faire à l'insu des collaborateurs (information, CE, syndicats ou représentants du personnel, etc.) ou envers une personne spécifique.

# La surveillance des activités

La surveillance concerne aussi des applications (fonctionnement, requêtes émises ou reçues, journal d'activité. . .).

## Attention CNIL

- S'il est possible de remonter à une personne à partir de ces données : cache de navigation avec authentification, journal des requêtes SQL avec id de la connexion. . .
- Aux traitements automatisés des traces d'activités.

Durée d'archivage préconisée : 1 an.

## Attention

Les journaux ou bases de données stockant ces informations doivent être protégés de manière particulièrement soigneuse (accès ou modifications illégitimes).

# Une question fréquente

## La DSI peut-elle donner des informations sur le surf d'un salarié ?

**Non**

Bertrand Braux , 01net., le 07/12/2007 à 17h30

C'est l'alinéa 2 de l'article 432-9 du Code pénal : l'administrateur a le droit « d'accéder » aux données personnelles, mais il ne peut les « intercepter ». La divulgation des contenus, y compris à la demande de son employeur, du dirigeant ou d'un responsable de service, ne relève pas des objectifs de sécurité du réseau et peut être sévèrement punie.

En revanche, il peut tout à fait, à la demande de son employeur, fournir les statistiques générales de tout un service : par exemple commercial...

[Retour au sommaire](#)

[http://www.01net.com/editorial/366219/la-dsi-peut-elle-donner-des-informations-sur-le-surf-d-un-salarie-./](http://www.01net.com/editorial/366219/la-dsi-peut-elle-donner-des-informations-sur-le-surf-d-un-salarie-/)