



L'INFORMATIQUE D'ENTREPRISE AU QUOTIDIEN

Droits, devoirs et usages

Cédric Cartau

2014

PRESSES DE L'ÉCOLE DES HAUTES ÉTUDES EN SANTÉ PUBLIQUE



Table des matières

Introduction.....	3
-------------------	---

PARTIE 1

Les usages de base

1. L'arrivée dans le système d'information.....	11
2. L'utilisation des matériels	15
Le PC.....	15
La configuration des PC et des autres matériels....	15
Du bon usage des supports d'échange de données.....	17
Du bon usage des outils de communication téléphonique.....	19
L'extinction électrique des matériels.....	20
3. Les moyens d'impression.....	23
Les technologies d'impression	23
Les économies de papier	24
La confidentialité des impressions.....	25
4. L'utilisation bureautique.....	27
Qu'est-ce que la bureautique?.....	27
Bureautique et sécurité.....	27
Les quotas.....	29
La sauvegarde des données.....	30
Les habilitations des partages de fichiers.....	31
5. Le départ du système d'information.....	33
L'absence temporaire.....	33
Le départ définitif.....	34

PARTIE 2

L'informatique d'entreprise en réseau

6. L'utilisation des logiciels métier	41
Logiciel ou progiciel?	41
Le respect des habilitations.....	41
Le non-détournement du fonctionnement initial.....	42
7. L'utilisation de la messagerie	45
La messagerie électronique.....	45
Les règles élémentaires de bienséance.....	46
Les implications juridiques.....	48
La messagerie et les automatisations	49
Les spams.....	52
8. L'utilisation des services Web	57
Les services d'Internet.....	57
Les espaces de stockage	57
Les messageries Web.....	61
Les systèmes de messagerie instantanée.....	61
Les réseaux sociaux.....	63
9. L'accès Internet	67
10. La gestion des fournisseurs	71

PARTIE 3

Les nouveaux enjeux

11. La mobilité	79
Qu'est-ce que la mobilité?.....	79
Le Wi-Fi.....	80
La gestion des déplacements en France et à l'étranger.....	81
Le télétravail.....	83

12. Le BYOD	87
Qu'est-ce que le BYOD?	87
Un concept protéiforme	87
Les aspects légaux.....	88
Le coût.....	90
Les vrais besoins.....	91
Les aspects techniques	92
De la permission à l'obligation.....	92
Les différents BYOD.....	93
13. La sécurité du système d'information	95
Garantir la sécurité du SI.....	95
Les fondamentaux.....	95
La hiérarchie des besoins.....	96
Les impacts sur les utilisateurs.....	97
La disponibilité, critère principal?	99
14. Les virus et malwares	103
Qu'est-ce qu'un virus?	103
Les évolutions.....	104
Les symptômes.....	105
La réaction.....	106

PARTIE 4

Les droits et devoirs de l'utilisateur

15. Le champ d'application	113
L'utilisateur.....	113
La notion d'administrateur.....	114
16. Les droits	115
La vie privée.....	115
Le règlement intérieur.....	116
Les opérations de contrôle.....	118
Le droit de disposer des outils permettant d'accomplir sa mission.....	123

17. Les devoirs	125
Les fondamentaux juridiques.....	125
Les principes d'accès.....	126
Les règles générales.....	128
Les règles spécifiques.....	134
18. Les cas particuliers	139
Les administrateurs système.....	139
Les organisations syndicales.....	141
Les fournisseurs.....	143
Conclusion	147
Les commandements	151
Liste des sigles	153
Annexes	155
Annexe 1. Les principaux arrêts de jurisprudence.....	155
Annexe 2. La responsabilité sous l'angle juridique.....	161

On trouve, dans les librairies spécialisées, bon nombre d'ouvrages sur l'informatique et les systèmes d'information. Qu'il s'agisse de configurer un serveur Linux, de monter un réseau Ethernet Gigabit ou de réaliser des macros sous Excel, le lecteur curieux n'a pas à chercher bien longtemps le livre adéquat. Dans ce domaine pourtant, le monde de l'édition est en chute libre : depuis la fin des années 2000, et surtout l'arrêt des innovations dans le domaine des langages de programmation, les rayons spécialisés des grandes enseignes s'étiolent à vue d'œil. Pour le voir, il suffit de se rendre dans cette enseigne grand public de Paris-Montparnasse et de tomber sur le pan de mur dédié à l'informatique, qui occupe à peine un carré de trois mètres sur trois alors qu'à la grande époque il aurait phagocyté quatre rayons entiers.

Cela dit, pour le lecteur avide d'informations, le Web fournit un nombre considérable de ressources techniques destinées au novice aussi bien qu'au professionnel. En parcourant les pages dédiés dans Wikipédia, on se rend compte à quel point l'information – et l'auto-formation – n'ont jamais été aussi accessibles qu'aujourd'hui. Sur des sujets aussi pointus que le cryptage asymétrique ou les technologies de VLAN, on trouve les bases des connaissances sans difficulté sur l'encyclopédie mondiale. Et pas simplement en anglais : même dans ce domaine technique, la plupart des pages sont traduites. Cette base

documentaire est classée par grandes catégories ou domaines techniques : les bases de données, les systèmes d'exploitation, les logiciels applicatifs, etc. De sorte que non seulement l'information est disponible, mais elle est facilement accessible : les moteurs de recherche sont nos amis et la seule saisie de la chaîne de caractères d'une erreur technique amène rapidement le lecteur à des blogs, des supports en lignes qui lui permettent de résoudre son souci.

Curieusement, dans cette masse documentaire, il est peu aisé de trouver des ouvrages dans l'esprit d'un guide pratique à destination du cadre d'entreprise et traitant de l'usage quotidien du système d'information : les précautions à prendre pour le choix d'un mot de passe, les règles élémentaires de protection contre les spams, etc. Or, si l'informatique dispose d'un socle conceptuel considérable et de technologies complexes pour les mettre en œuvre, la vie de l'utilisateur en entreprise est souvent éloignée de cette complexité : les préoccupations du cadre sont souvent très terre à terre vis-à-vis de cet outil, il attend que cela fonctionne et qu'on lui en explique les usages principaux en termes simples et accessibles.

Il existe beaucoup de points communs entre l'usage courant de l'informatique en entreprise, et l'utilisation de ces mêmes outils dans la sphère domestique : la bureautique utilise les mêmes outils, les virus attaquent sans discernement. Utiliser Open Office à la maison et enregistrer ses fichiers dans un format odt ou les exporter dans un format pdf ne diffèrent en rien, que l'on se trouve au bureau ou dans son salon. Ces technologies ou outils spécifiques sont en fait utilisés à des fins de bureautique basique la plupart

du temps. Il existe aussi nombre de différences qui rendent impossible une comparaison point à point : l'espace disque est quasi infini à la maison, il est coûteux en entreprise, la messagerie professionnelle est beaucoup plus cadrée dans les usages que la messagerie personnelle, etc.

Il paraît donc utile de rassembler, au sein d'un même ouvrage, la somme des connaissances nécessaires à l'usager courant : l'utilisation des principaux outils, les règles de bon usage, les erreurs à éviter, mais aussi les droits et le devoir de l'usager face au système d'information. Publier un commentaire sur un blog depuis chez soi n'a pas la même incidence que de le faire depuis son lieu de travail et pendant les heures de bureau. Les accès Internet n'obéissent pas non plus aux mêmes contraintes de traçabilité et de filtrage.

Cet ouvrage ne constitue pas un cours de système d'information. Il existe pour cela des ouvrages spécialisés, le lecteur intéressé pourra consulter à ce titre les bibliographies en fin de parties. Il s'agit d'un guide pratique, à destination du cadre d'entreprise ou de toute personne confrontée au quotidien à l'usage de l'outil informatique – autant dire presque tout le monde de nos jours. Dans le propos traité, la fonction de cadre englobe aussi bien l'encadrant que ses subordonnés, pour qui l'usage de l'informatique est un outil de travail. Il a été constitué à partir de différentes sources : chartes utilisateur, guide de bon usage, corpus juridique, etc. Le propos est certes technique, mais à des fins de vulgarisation autant que possible. Dans la plupart des cas, nous avons essayé de relier les notions les plus complexes à des exemples de la vie courante.

La première partie traite des usages basiques de l'informatique dans l'entreprise : arrivée de l'agent dans l'entreprise, utilisation des matériels et logiciels, etc.

La deuxième partie aborde des usages en réseau : logiciels métier, accès Internet, bon usage de la messagerie, etc.

Dans la troisième partie, nous exposerons des nouveaux enjeux de l'informatique d'entreprise : la mobilité, le BYOD, la sécurité des informations.

La quatrième partie a pour objet les droits et les devoirs de l'utilisateur du système d'information, essentiellement au regard des contraintes réglementaires.

L'ouvrage peut aussi bien être lu de façon séquentielle – du début à la fin – qu'en allant directement au chapitre concerné.

Le lecteur trouvera une bibliographie et des sites Internet à la fin de chaque partie et des annexes en fin d'ouvrage traitant de certains aspects juridiques de l'usage de l'informatique en entreprise.

“J’ai toujours rêvé d’un ordinateur qui soit aussi facile à utiliser qu’un téléphone. Mon rêve s’est réalisé : je ne sais plus comment utiliser mon téléphone.”

B. Stroustrup

Les usages de base

1

PARTIE

L'informatique est un outil complexe, *a fortiori* en entreprise. Les mésusages sont la plupart du temps dus à l'absence de connaissance des règles élémentaires, il est en effet très rare de constater un incident dû à la malveillance.

Cette partie balaye l'ensemble des règles de base – que nous pourrions qualifier de « bonne hygiène » – qu'il convient de connaître et de respecter pour tirer partie au mieux de l'outil informatique.



L'arrivée dans le système d'information

1

La **DSI** est le service interne de l'entreprise qui est chargé de gérer l'informatique.

À l'arrivée dans l'établissement, l'agent se voit doter d'un certain nombre de moyens techniques : carte de parking, badge d'accès aux locaux, bureau, etc. La DSI lui attribue également des moyens informatiques : accès aux applications métier, boîte aux lettres de messagerie électronique, et surtout un mot de passe temporaire d'accès à sa session (la plupart du temps une session Windows).

Ce mot de passe doit être changé à la première connexion : peu de personnes savent correctement choisir le leur et optent généralement pour le prénom de leur grand-mère ou la date d'anniversaire de leur conjoint (voire une combinaison des deux). Le choix d'un mot de passe est important car :

- l'utilisation des moyens individuels (messagerie électronique, accès individuel à un logiciel métier) engage la responsabilité juridique de son détenteur ; dans le cas où l'agent prêterait son mot de passe à un collègue, il doit savoir qu'il sera redevable des éventuelles « bêtises » que pourrait faire le collègue en question ;

- un mot de passe se découvre (se « cracke ») d'autant plus facilement qu'il est simple.

1

Les pirates ne sont pas les seuls à disposer de programmes spéciaux pour découvrir les mots de passe : on trouve ce genre d'outils très facilement sur Internet, une simple recherche dans Google ramène des liens très instructifs.

Ces programmes fonctionnent soit sur la base de la « force brute » (qui consiste à essayer toutes les combinaisons), soit à partir de dictionnaires de mots. Dans tous les cas, on peut considérer que :

- un mot de passe de 8 caractères utilisant tout l'alphabet peut être cracké en moins de 5 minutes ;
- un mot de passe de 8 caractères utilisant l'alphabet (majuscules et minuscules) ainsi que les chiffres nécessite plusieurs jours pour être cracké ;
- un mot de passe de 8 caractères utilisant l'alphabet (majuscules et minuscules), les chiffres et les caractères spéciaux (ponctuation, /, & ; ...) nécessite plusieurs mois pour être cracké.

Un bon mot de passe doit obéir aux règles suivantes :

- être d'une longueur de 8 caractères au moins ; dans le cas de mots de passe sensibles (par exemple ceux permettant d'accéder à des données très confidentielles), il faut 10 voire 12 caractères de long ;
- mélanger majuscules et minuscules, lettres, chiffres et caractères spéciaux ;
- ne pas figurer dans un dictionnaire : il faut éviter d'utiliser des noms communs ;
- ne pas être commun à plusieurs comptes utilisateurs : par exemple, si l'agent dispose d'une messagerie personnelle à son domicile, il ne faut jamais choisir le même mot de passe pour cette messagerie que pour son compte Windows professionnel ; de nombreux cas de piratage ont pour origine ce choix identique.