

TABLE DES MATIÈRES

INTRODUCTION.....	1
PARTIE 1. Les justifications des employeurs pour cybersurveiller les salariés.....	7
Chapitre 1. L'impératif de sécurité informatique.....	11
Section 1. La nécessaire protection du réseau informatique.....	12
1.1 Les risques d'atteinte à la sécurité et à la confidentialité des données.....	12
1.2 L'obligation de sécurité et de confidentialité des données.....	16
1.2.1 Définition de l'obligation de sécurité et de confidentialité des données.....	16
1.2.2 Portée de l'obligation de sécurité et de confidentialité des données.....	19
1.2.2.1 Une obligation de moyens.....	19
1.2.2.2 Des sanctions financières parfois lourdes.....	21
Section 2. L'admission de l'impératif de sécurité comme motif légitime de surveillance.....	24
Chapitre 2. La répression des abus.....	29
Section 1. L'obligation d'exécuter le travail avec prudence et diligence.....	31

1.1	Le devoir d'obéissance.	31
1.2	La productivité	35
1.3	La sécurité des biens et équipements professionnels	43
Section 2.	L'obligation de loyauté et de discrétion	45
2.1	L'obligation de confidentialité	47
2.2	L'obligation d'exclusivité et de fidélité	51
2.3	La préservation de la réputation et de l'image de l'entreprise	53
Chapitre 3.	Les risques de responsabilité.	61
Section 1.	Les fondements de la responsabilité de l'employeur.	62
1.1	La responsabilité du commettant	63
1.2	L'influence de la qualité de fournisseur d'accès Internet de l'employeur sur le régime de responsabilité applicable	72
Section 2.	Les principaux motifs de responsabilité	81
2.1	Les atteintes aux droits de la personne.	82
2.2	Les atteintes à la confidentialité et aux droits de propriété intellectuelle.	89
Section 3.	Les possibilités de limitation ou d'exonération de responsabilité.	92
3.1	L'absence de contrôle du commettant	94
3.2	L'absence de lien entre la faute du préposé et l'exécution de ses fonctions.	97
Conclusion	de la première partie	101

PARTIE 2. L'encadrement juridique de la surveillance des ressources informatiques fournies pour le travail	103
Chapitre 1. L'existence de directives d'utilisation des ressources informatiques claires	109
Section 1. Les politiques d'utilisation de l'Internet	110
1.1 Le contenu des politiques Internet	111
1.2 Les critères de validité des politiques Internet	113
1.2.1 La connaissance de la politique par les salariés	114
1.2.2 L'utilisation d'un langage clair et sans équivoque	115
1.2.3 L'application constante et uniforme de la politique	115
1.2.4 L'information des salariés sur les consé- quences du non-respect de la politique	116
1.2.5 Le caractère raisonnable de la politique	118
1.2.6 La conformité de la politique aux dispo- sitions législatives et réglementaires	119
1.3 L'impact juridique de la politique Internet	119
1.3.1 La possibilité de discipliner efficacement les salariés	120
1.3.2 La limitation de la responsabilité de l'employeur	123
1.3.3 La limitation de l'expectative de vie privée des salariés	123
Section 2. Les clauses contractuelles	126

Chapitre 2. L'existence d'un intérêt sérieux et légitime	131
Section 1. L'exigence d'un motif de surveillance raisonnable et probable	134
1.1 L'existence d'un problème important, réel et précis	134
1.1.1 Le caractère sérieux du motif	135
1.1.2 L'impact des facteurs aggravants ou atténuants	138
1.1.2.1 La nature de l'emploi du salarié ou de l'activité de l'organisation	139
1.1.2.2 Le dossier disciplinaire du salarié, le niveau de gravité de ses manques et son comportement après la découverte des faits	143
1.2 Le lien avec les exigences du bon fonctionnement de l'entreprise	147
1.3 L'antériorité du motif de la surveillance	148
Section 2. La proportionnalité et la pertinence de la surveillance	152
Section 3. L'étendue de l'atteinte à la vie privée	156
3.1 La notion de vie privée au travail	156
3.2 La prise en compte concrète de l'expectative de vie privée lors de l'accès au contenu de l'ordinateur du salarié	162
3.2.1 La nature des renseignements protégés.	162
3.2.2 L'auteur de la fouille de l'ordinateur du salarié	170
3.2.3 L'étendue de la fouille de l'ordinateur du salarié	172

Conclusion de la deuxième partie	175
PARTIE 3. La surveillance des activités des salariés sur les médias sociaux	179
Chapitre 1. <i>Facebook</i> , une pièce à conviction de choix pour les employeurs.	183
Section 1. <i>Facebook</i> est un espace public...	186
Section 2. ... Où même les contenus à « diffusion restreinte » peuvent justifier un congédiement	194
Chapitre 2. La légitimité de l'utilisation des contenus publiés sur les médias sociaux à l'encontre du salarié.	201
Section 1. Les contenus justifiant des sanctions disciplinaires.	202
1.1 Atteintes à la réputation de l'employeur.	203
1.2 Harcèlement psychologique	207
1.3 Absences frauduleuses et déclarations d'invalidité mensongères	210
Section 2. La légalité de l'interception des propos du salarié.	214
3.1 L'accès aux propos du salarié.	214
3.1.1 La légalité des moyens d'accès aux propos du salarié	214
3.1.2 La légitimité des motifs d'accès aux propos du salarié	217
3.2 L'ampleur de la fouille dans le profil du salarié.	219
3.3 La possible admission de preuves obtenues en violation d'un droit fondamental du salarié	222

Section 3. Le recours à des politiques d'utilisation des réseaux sociaux	225
Conclusion de la troisième partie	227
CONCLUSION	231
Annexe I. Aide-mémoire sur Internet – Utilisation du matériel informatique de l'employeur	235
Annexe II. Aide-mémoire sur Internet – Utilisation des médias sociaux en dehors du cadre du travail	237
Annexe III. Tableau des manquements liés à l'usage des ressources informatiques mises à la disposition des salariés et mesures appliquées	239
Annexe IV. Tableau des décisions jurisprudentielles concernant la surveillance des salariés sur les médias sociaux	257
BIBLIOGRAPHIE	273
TABLE DE LA LÉGISLATION	289
TABLE DE LA JURISPRUDENCE	293
INDEX ANALYTIQUE	305