

Guide juridique Informatique et Libertés

Collecte, traitement et sécurité des données
dans l'univers numérique : ce que vous devez savoir

Gérard HAAS
Yaël COHEN-HADRIA



Marketing

BOOK



جامعة أمحمد بوقرة - بومرداس
Université M'hamed Bougara - Boumerdes
المكتبة الجامعية
رقم الجرد: 0103 975

Guide juridique Informatique et Libertés

Collecte, traitement et sécurité des données
dans l'univers numérique : ce que vous devez savoir

جامعة أمحمد بوقرة - بومرداس
المكتبة الجامعية
Université M'hamed Bougara - Boumerdes
Exercice: 2014
Fournisseur: Eclat hab
N° Facture: 141210037
Position de Titre: 144
N° d'inventaire: 0103 975

جامعة أمحمد بوقرة - بومرداس
Université M'hamed Bougara - Boumerdes
المكتبة الجامعية
رقم: 004.43/HAD
01EX

Avant-propos

Chapitre 1

La loi Informatique et libertés

A. Introduction	9
B. Pourquoi une loi de 1978 est-elle autant d'actualité sur Internet ?	9
1. Loi Informatique et libertés & Démocratisation d'Internet	9
2. Protection de la vie privée & loi Informatique et libertés	13
3. Rayonnement de la protection des données en Europe	17
4. Vers une harmonisation des régimes de protection des données à caractère personnel	21
a. Sources du régime de protection des données à caractère personnel	21
b. Harmonisation à l'échelle communautaire	21
c. Travail du G29	24
d. Harmonisation à l'échelle internationale	26
e. Travail des membres de la Conférence Internationale des Commissaires à la Protection des Données et à la Vie Privée	27
C. CNIL : garante du respect de la loi Informatique et libertés	28
1. Autorité Administrative Indépendante (AAI)	28
2. Budget	29
3. Nombre de postes	30
4. Composition	31
5. Organisation	32
6. Formations	33
7. Missions	34
8. Pouvoirs	35
a. Informer les personnes	36
b. Autoriser les traitements de données à caractère personnel	38
c. Émettre des avis	39
d. Délibérer	40
e. Force de proposition au Gouvernement	42
f. Contrôler	43
g. La CNIL en chiffres	48
D. Qu'avez-vous retenu de ce chapitre ?	51

Chapitre 2

Notions fondamentales et loi Informatique et libertés

A. Applicabilité de la loi Informatique et libertés	55
1. Critère matériel	55
a. Notion de « données à caractère personnel »	55
b. Notion de « traitement »	56
2. Champ fonctionnel	56
3. Champ territorial	58
a. Critère lié à l'établissement de la personne sur le territoire français	58
b. Critère de territorialité des moyens utilisés	58
c. Exclusions des copies temporaires	59
d. Loi Informatique et libertés : pas une loi de police	59
4. Synthèse	60
B. Acteurs de la loi Informatique et libertés	61
1. Responsable de traitements	62
2. Destinataire	63
3. Sous-traitant	64
4. Personnes concernées	64
5. Correspondant Informatique et libertés (CIL)	65
a. Rôle et mission du CIL	65
b. Choix du CIL	67
6. Synthèse	71
C. Données sensibles	72
1. Données interdites	73
2. Infractions, condamnations et mesures de sureté	75
3. Numéro de sécurité sociale	77
4. Appréciation des difficultés sociales des personnes	78
D. Formalités préalables	79
1. Dispense de formalités préalables	80
2. Déclaration simplifiée	80
3. Déclaration	81
4. Demande d'autorisation	81
5. Demande d'avis	83
E. Licéité des traitements de données à caractère personnel	85
1. Licéité des données	85
2. Licéité de la collecte	86

F. Consentement des personnes concernées	87
1. Définition de la notion de consentement	88
2. Exception au recueil du consentement	89
G. Information des personnes	89
1. Contenu de l'information	90
2. Modalités de l'information	90
H. Synthèse des fondamentaux	91
I. Qu'avez-vous retenu de ce chapitre ?	92

Chapitre 3

Enjeux d'une collecte loyale des données sur Internet

A. Enjeux pour l'entreprise présente sur les réseaux sociaux	97
1. Réseaux sociaux : un vivier de données à caractère personnel	97
a. Qu'est-ce qu'un réseau social	97
b. Obligations du titulaire du réseau social en ligne	98
c. Droits des utilisateurs	99
2. Licéité de la collecte par une entreprise des données présentes sur les réseaux sociaux	100
a. Accessibilité des données	100
b. Réutiliser les données des membres des réseaux sociaux	101
c. Stratégie digitale : collecte des données des fans	106
3. Respect de la vie privée et droit à l'oubli	107
a. Définition du droit des personnes	107
b. Origine du droit à l'oubli	108
c. Consécration d'un droit à l'oubli sur Internet ?	109
d. Compétence des juges français	110
B. Enjeux pour l'entreprise qui rachète des bases de données	113
1. Pré-requis au rachat d'une base de données	113
a. Définition des besoins de l'entreprise acheteuse	114
b. Audit de la base de données au regard de la loi	115
2. Sécuriser le rachat d'une base de données	115
a. Précautions particulières	115
b. Aspects contractuels	116
C. Utilisation des données à des fins commerciales	116
1. Cadre légal et best practices applicables à toute utilisation de données à des fins commerciales	117
a. Définition	117
b. Intérêt de cette pratique	118

c. Régime juridique	118
2. Cadre légal et best practices spécifiques par canal	120
a. Best practices en matière d'e-mailing	120
b. Best practices en matière de cookies	128
c. Best practices en matière de retargeting	134
d. Best practices en matière de géolocalisation	139
D. Qu'avez-vous retenu de ce chapitre ?	144

Chapitre 4

Sécuriser et protéger vos données

A. Obligation générale de protection des données	149
1. Obligation de résultat ou obligation de moyens renforcée ?	149
a. Obligation générale de sécurité	149
b. Risques liés à la nature des données	150
c. Risques liés au traitement	151
d. Gestion des risques : une appréciation au cas par cas	152
e. 10 conseils de la CNIL en matière de sécurité	154
f. Sous-traitant : mesures particulières	156
g. Exemples de procédés de sécurisation des données	157
h. Cas particulier des données de santé	159
2. Risques et sanctions	162
3. Délibérations de la CNIL en matière de sécurité	163
4. Notification des failles de sécurité	166
a. Contenu de cette obligation de notification	167
b. Caractère absolu de l'obligation de notification	167
c. Modalités concrètes de la notification à la CNIL	168
d. Modalités de notification aux personnes physiques	168
e. Tenue d'un registre des violations	169
f. Risques et sanctions	170
B. Outils pour la sécurité des données	170
1. Obligations de l'employeur/responsable de traitement	170
2. Outils de protection des risques sécuritaires au sein de l'entreprise	172
a. Sécurité des locaux	172
b. Sécurité des réseaux	173
c. Sécurité des serveurs et des applications	173

3. Outils de prévention des risques sécuritaires au sein de l'entreprise	174
a. Cartographier les flux et définir des profils d'habilitation des utilisateurs du système	174
b. Mettre en place des contrôles	175
c. Sensibiliser les utilisateurs	175
4. Outils offensifs relatifs aux risques de sécurité	177
a. Action pénale fondée sur les articles 226-16 et suivants du Code pénal	177
b. Action pénale fondée sur les articles 323-1 et suivants du Code pénal	177
c. Action pénale fondée sur les articles 323-1 et suivants du Code pénal	178
5. Cas particulier d'une Privacy Policy sur Internet	179
a. Stratégie de marketing digital	179
b. Contenu de la « Privacy Policy »	184
c. Gage de confiance	185
d. Gage d'optimisation des coûts	186
e. Gage de bonne foi	186
C. Qu'avez-vous retenu de ce chapitre ?	188

Chapitre 5

Sécurité des transferts de données

A. Identification et conditions de licéité d'un flux transfrontières de données	193
1. Identification et régime applicable	193
a. Flux entrants	193
b. Flux transfrontières	194
2. Application des principes généraux de licéité des traitements	198
3. Formalités préalables	199
4. Information des personnes	202
5. Contractualisation des flux transfrontières de données à caractère personnel	203
a. Transfert « hors groupe »	204
b. Transferts « intra-groupe »	205
B. Particularité du Cloud Computing	206
1. Pourquoi le Cloud Computing ?	206
a. Engouement international	206
b. Terminologie	207
c. Fonctionnement	207
d. Typologie	209
e. Intérêt	210
f. Inquiétudes	211