

AIDE-MÉMOIRE DE DROIT À L'USAGE DES RESPONSABLES INFORMATIQUE

Isabelle Renard

Avocat associée du Cabinet Racine

Jean-Marc Rietsch

Président de FedISA

DUNOD

Toutes les marques citées dans cet ouvrage sont des marques déposées par leurs propriétaires respectifs.

La dématique® correspond à l'action de dématérialiser au sens large, elle touche à la fois la numérisation de documents papiers, la dématérialisation des échanges et la dématérialisation des processus en y incluant la composante légale (source : www.fedisa.eu).

Maquette de couverture : Mateo

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage. Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements	d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée. Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).
	

© Dunod, Paris, 2012
ISBN 978-2-10-057946-4

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

Avant-propos	XI
Chapitre 1 – RSI – De quoi êtes-vous responsables ?	1
1.1 Quels sont les risques pour les RSI ?	1
1.2 Le contexte de la mise en œuvre de la responsabilité du RSI ..	2
1.2.1 Définition	2
1.2.2 La responsabilité civile	3
1.2.3 La responsabilité pénale	8
1.2.4 Le préjudice subi par l'entreprise du fait de son SI	13
1.3 Recommandations	14
Chapitre 2 – Le patrimoine incorporel de l'entreprise	15
2.1 Les enjeux	15
2.2 Le contexte	17
2.2.1 La protection du logiciel	17
2.2.2 La protection des créations intellectuelles (hors logiciel)	24

2.2.3	<i>La protection des bases de données</i>	26
2.2.4	<i>Les activités de recherche – le savoir-faire</i>	28
2.2.5	<i>La protection technique des données du patrimoine informationnel ou « data leak protection »</i>	29
2.3	<i>Recommandations</i>	37
Chapitre 3 – Téléchargements illicites et loi Hadopi		39
3.1	<i>Les enjeux de la loi Hadopi pour l'entreprise</i>	39
3.2	<i>Le contexte</i>	40
3.2.1	<i>Qu'est-ce que l'Hadopi ?</i>	40
3.2.2	<i>La loi Hadopi</i>	40
3.2.3	<i>Les obligations de l'entreprise en tant que titulaire de l'accès Internet</i>	41
3.2.4	<i>Les applications judiciaires de la loi Hadopi en entreprise</i>	43
3.3	<i>Recommandations</i>	43
3.3.1	<i>Se munir des moyens techniques de prévention</i>	43
3.3.2	<i>Prévoir la mise à jour de la déclaration CNIL</i>	44
3.3.3	<i>Mettre à jour ou élaborer la charte informatique</i>	45
Chapitre 4 – Gérer les intervenants sur le SI		47
4.1	<i>Les enjeux</i>	47
4.1.1	<i>Éditeurs et prestataires</i>	47
4.1.2	<i>Faire la différence entre les salariés de l'entreprise et les autres intervenants</i>	49
4.1.3	<i>Avantages et inconvénients des contrats types</i>	50
4.2	<i>Le contexte</i>	52
4.2.1	<i>Les contrats informatiques : ce qu'il faut savoir</i>	52
4.2.2	<i>Contrats de projet et relations sur le long terme</i>	64
4.2.3	<i>Les pièges des contrats de « régie »</i>	68
4.2.4	<i>La sous-traitance</i>	70

4.2.5	<i>Peut-on se débarrasser du jour au lendemain d'un prestataire ?</i>	72
4.2.6	<i>Les contrats internationaux</i>	73
4.2.7	<i>Les contrats peuvent-ils être conclus par voie électronique ?</i>	73
4.3	<i>Recommandations</i>	74
Chapitre 5 – Encadrer les pratiques des salariés		77
5.1	<i>Les enjeux</i>	77
5.2	<i>Le contexte</i>	79
5.2.1	<i>Les précautions liées à la protection des données personnelles</i>	79
5.2.2	<i>Le cas particulier des activités illégales</i>	81
5.2.3	<i>Petit aperçu de jurisprudence</i>	83
5.2.4	<i>La charte informatique</i>	85
5.3	<i>Recommandations</i>	86
Chapitre 6 – Les données personnelles		87
6.1	<i>Les enjeux</i>	87
6.2	<i>Le contexte</i>	88
6.2.1	<i>L'environnement juridique général</i>	88
6.2.2	<i>L'obligation de sécurité</i>	91
6.2.3	<i>Accès à la messagerie et aux fichiers des salariés : où en est-on ?</i>	95
6.2.4	<i>Le cas particulier de l'accès aux dossiers et mails du salarié ayant quitté l'entreprise ou décédé</i>	99
6.2.5	<i>Les dispositifs d'alerte professionnelle de dénonciation ou « whistleblowing »</i>	102
6.2.6	<i>Les transferts internationaux de données personnelles</i>	104
6.2.7	<i>La position de la CNIL en matière d'archivage numérique</i>	107
6.3	<i>Recommandations</i>	111

Chapitre 7 – Conservation et processus numériques	113
7.1 Les enjeux	113
7.2 Le contexte	115
7.2.1 Les aspects juridiques	115
7.2.2 Dématique	124
7.2.3 Archivage électronique, importance du cycle de vie des documents	128
7.3 Recommandations	132
 Chapitre 8 – L'impact des comptabilités informatisées sur le SI ..	 135
8.1 Les enjeux	135
8.2 Le contexte	137
8.2.1 Un cadre réglementaire actualisé depuis 2006	137
8.2.2 Établir une cartographie des applications	141
8.2.3 Les obligations relatives à la documentation	142
8.2.4 Les obligations relatives à l'archivage des documents et données	143
8.2.5 Normes de conservation de données comptables	145
8.2.6 Les précautions contractuelles indispensables	145
8.2.7 La délocalisation ne règle pas le problème	147
8.2.8 Migration matérielle ou logicielle	147
8.2.9 Impact de la certification NF 203	147
8.2.10 Les modalités du contrôle de la comptabilité informatisée	148
8.2.11 Les normes IFRS (International Financial Reporting Standards)??	149
8.3 Recommandations	150
 Chapitre 9 – Comment faire face aux situations de e-discovery ? .	 153
9.1 Les enjeux de « e-discovery »	153

9.2	Le contexte du « e-discovery » en France	155
9.2.1	Le e-discovery US : conséquences en France	155
9.2.2	Les investigations sur le SI dans le cadre d'une procédure pénale	157
9.2.3	Les investigations sur le SI dans le cadre d'une procédure civile	158
9.2.4	Les saisies dans le cadre des enquêtes sur les pratiques anticoncurrentielles	160
9.2.5	Les enquêtes de l'AMF (Autorité des marchés financiers) ...	161
9.3	Recommandations pour se préparer au e-discovery	162
9.3.1	Quelle information conserver ?	162
9.3.2	Pendant combien de temps conserver ?	163
9.3.3	Comment conserver ?	164
9.3.4	Comment supprimer ?	164
9.4	Un exemple vécu de « pré-discovery »	166
9.5	Recommandations	169
Chapitre 10	Le cloud computing	171
10.1	Les enjeux	171
10.2	Le contexte	172
10.2.1	Une grande diversité	172
10.2.2	La question de la sécurité	173
10.2.3	Limites à l'utilisation du cloud computing liées au type de données	175
10.2.4	Cloud computing et e-discovery	176
10.2.5	Les données personnelles dans le cloud	176
10.2.6	Le contexte contractuel du cloud computing	179
10.2.7	Impact de la normalisation	182
10.2.8	Peut-on utiliser le cloud computing pour mettre en place un système d'archivage numérique ?	183
10.3	Recommandations	185

Chapitre 11 – Traitement assurantiel : de l’anticipation à la réparation	187
11.1 Les fondamentaux de l’assurabilité	187
11.2 Le contexte de l’assurance des systèmes d’information en France	189
11.3 Recommandations	191
11.3.1 <i>Mise en place de programmes d’assurance des systèmes d’information</i>	191
11.3.2 <i>Un exemple vécu de sinistre</i>	195
11.3.3 <i>Quelles couvertures du risque pourraient être envisagées pour couvrir le détenteur d’information ?</i>	197
11.3.4 <i>Design des programmes d’assurances</i>	199
Glossaire	201
Webographie	203
Index	205

Avant-propos

Qu'il soit DSI¹ ou RSSI², celui que nous appellerons de façon générique responsable de système d'information, ou « RSI » est le gardien de l'information avec un grand « I », puisque cette information est de plus en plus riche et structurante du patrimoine de l'entreprise. Le RSI s'interroge à juste titre sur ses risques et ses responsabilités, et ce d'autant que son métier s'est considérablement complexifié ces dernières années, du fait de plusieurs facteurs.

Le premier de ces facteurs est celui de la multiplication des offres de service externalisées. Le système d'information n'a plus un périmètre fermé et maîtrisable, auquel il suffirait d'ajouter les remparts permettant de se protéger des attaques extérieures. Les RSI doivent passer de la gestion de la sécurité à la gestion du risque, et assumer le fait que le risque zéro n'existe pas. Les offres de service externalisées permettent l'accès à des ressources sophistiquées, mais elles complexifient le périmètre fonctionnel du système d'information et étendent sa localisation géographique de façon incontrôlable. L'exemple le plus récent en est le *cloud* dans sa version SaaS (*Software as a Service*).

Le deuxième facteur concerne la multiplication des réglementations qui ont un impact sur le système d'information, et qui ont vocation à réguler un secteur d'activités, une fonction de l'entreprise,

1. Directeur des systèmes d'information.

2. Responsable de la sécurité des systèmes d'information.

ou encore comme récemment à travers la loi Hadopi, de sanctionner l'entreprise pour des comportements de ses utilisateurs. Il est difficile de demander à un responsable de système d'information, qui souvent n'a aucune formation juridique, de connaître toutes ces réglementations et surtout d'en apprécier l'impact. Or, la méconnaissance de ces règles peut avoir des conséquences lourdes pour l'entreprise dans des situations de plus en plus fréquentes où le système d'information fait l'objet d'audits et de demandes de production forcée de type *discovery*.

Le troisième facteur est la difficulté à maîtriser tant les utilisateurs du système d'information que ses acteurs. Les utilisateurs peuvent créer de graves dommages aux tiers et à l'entreprise par des comportements inappropriés. Quant aux nombreux sous-traitants et prestataires qui interviennent sur le système d'information, que ce soit en administration, en maintenance applicative ou en développement, ils sont liés à l'entreprise par des contrats qui sont parfois très peu protecteurs des intérêts de l'entreprise.

Objectif et organisation de l'ouvrage

L'objectif que nous nous sommes fixé dans cet ouvrage consiste à présenter au RSI son environnement de risque et à lui donner les clés qui lui permettront de l'évaluer de façon réaliste. Bien gérer le risque, n'est-ce pas déjà bien le connaître ?

Les différents chapitres de cet ouvrage peuvent être vus comme des fiches indépendantes dont l'objectif est de décrire les aspects de l'état de l'art qui ne sont pas strictement technologiques, pour donner au RSI les bases qui lui permettront de se les approprier dans le contexte qui est plus précisément le sien, et exercer ainsi son métier de la façon la plus éclairée possible.

À cette fin, nous aborderons tout d'abord la signification juridique du terme « responsabilité », qui a un sens différent dans le langage courant et dans le langage juridique, et est souvent mal compris et/ou mal interprété. Responsabilité pénale, civile, disciplinaire, que risque réellement le responsable du SI ?

Nous verrons que le RSI doit de se conduire en « bon père de famille » de sa profession afin de limiter son risque. Cela implique de bien connaître l'environnement légal et réglementaire ayant un impact sur le système d'information, ce qui n'est pas une mince affaire dans une époque qui légifère et réglemente à tour de bras,

souvent à la hâte. Nous présenterons les principales réglementations qui s'appliquent au système d'information, selon deux grandes parties, les règles de bases et les principales contraintes réglementaires. Pour une meilleure accessibilité, chacune de ces parties a été découpée en chapitres traitant d'un sujet précis et se terminant par des recommandations associées :

- **I) Les règles de bases (chapitres 1 à 5)** – La première partie de l'ouvrage s'attache aux règles de base en matière de protection du patrimoine informationnel de l'entreprise, comprenant, outre les notions juridiques concernant le logiciel et les créations intellectuelles, les recommandations pour contrôler les utilisateurs du SI, maîtriser les intervenants, et savoir organiser de façon professionnelle les archives numériques de l'entreprise.
- **II) Les principales contraintes en matière de conformité (chapitres 6 à 9)** – La deuxième partie présente les principales contraintes de conformité : protection des données personnelles, contrôle fiscal des comptabilités informatisées et situations de *e-discovery*. Les réglementations sectorielles spécifiques (telles que celles liées au secteur pharmaceutique ou au secteur bancaire) ne sont pas abordées dans cet ouvrage.

Nous terminerons par un sujet impossible à ne pas aborder de nos jours, celui du *cloud computing*, objet du chapitre 10 et en abordant un aspect non moins important des risques, celui de l'assurance au chapitre 11.

Cet ouvrage ne prétend pas à l'exhaustivité : il plante le décor général, déjà fort chargé, de l'environnement juridique du système d'information. Nous souhaitons que sa lecture rende les choses non pas plus compliquées mais plus simples, en donnant au RSI les clés essentielles pour aborder les aspects non strictement techniques de son métier.

Un glossaire et un index détaillé figurent en fin d'ouvrage.

À qui s'adresse ce livre ?

Cet ouvrage s'adresse aux responsables de système d'information, appellation qui recouvre des métiers très divers selon qu'elle vise