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

ISBN 978-2-10-057946-4

Table des matières

Avant-propos

Qu'il soit DSI[1] ou RSSI[2], 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