

TABLE DES MATIÈRES

| | |
|---|----|
| INTRODUCTION..... | 1 |
| I. LA QUALIFICATION DE L'OBLIGATION DE SÉCURITÉ INFORMATIONNELLE | 13 |
| A. La sécurité informationnelle : une définition | 13 |
| <i>Figure 1 : Relation entre la sécurité et le danger</i> | 13 |
| 1. La création des risques..... | 23 |
| a) La disponibilité (ou l'accessibilité) des données | 24 |
| <i>Figure 2 : Continuum disponibilité – sécurité</i> | 25 |
| b) L'intégrité des données | 26 |
| c) La confidentialité des données | 27 |
| 2. La gestion des risques | 33 |
| <i>Figure 3 : Processus de gestion des risques</i> | 34 |
| a) Les vulnérabilités..... | 35 |
| b) Les menaces | 39 |
| c) Les contre-mesures | 41 |
| d) Les valeurs (actifs)..... | 44 |
| B. L'analyse de risque comme vecteur de l'obligation de sécurité | 47 |
| 1. Le processus d'analyse de risque..... | 48 |

| | |
|--|-----|
| a) L'identification de la valeur des informations à protéger | 51 |
| b) L'identification des vulnérabilités et des menaces. | 54 |
| <i>Figure 4 : Relation entre l'impact et la probabilité d'une menace.</i> | 55 |
| c) L'évaluation de la probabilité qu'une menace ait des incidences juridiques pour l'entreprise. | 56 |
| (i) L'analyse quantitative | 57 |
| <i>Figure 5 : Schéma des brèches de sécurité.</i> | 60 |
| (ii) L'analyse qualitative. | 61 |
| <i>Tableau 1 : Échelles de qualification des événements dommageables</i> | 63 |
| <i>Tableau 2 : Niveaux de criticité.</i> | 63 |
| d) Comment établir un équilibre économique entre les dommages et le coût des contre-mesures. | 64 |
| 2. Le cadre juridique de l'analyse de risque | 68 |
| a) L'évaluation des risques comme obligation législative | 72 |
| b) L'adoption de politiques de sécurité comme obligation législative | 75 |
| II. LE CADRE JURIDIQUE DE L'OBLIGATION DE SÉCURITÉ INFORMATIONNELLE. | 87 |
| A. L'étendue de l'obligation de sécurité informationnelle | 88 |
| 1. L'intensité de l'obligation de sécurité informationnelle | 95 |
| a) Les dispositions législatives fondant l'obligation de sécurité informationnelle | 101 |

| | | |
|-------|---|-----|
| (i) | L'article 10 de la <i>Loi sur la protection des renseignements personnels dans le secteur privé</i> | 101 |
| (ii) | L'article 25 de la <i>Loi concernant le cadre juridique des technologies de l'information</i> | 102 |
| (iii) | L'article 1457 C.c.Q. | 105 |
| (iv) | L'article 4.7 du Code type sur la protection des renseignements personnels | 107 |
| b) | L'intensité relative de l'obligation de sécurité | 110 |
| (i) | L'obligation de moyens renforcée | 111 |
| (ii) | L'obligation de résultat atténuée | 113 |
| 2. | La qualification du RSI « raisonnablement prudent et diligent » | 118 |
| a) | Les normes de l'industrie. | 119 |
| b) | L'industrie des normes. | 128 |
| B. | Les balises juridiques de l'obligation de sécurité informationnelle | 138 |
| 1. | Les balises législatives de l'obligation de sécurité informationnelle | 139 |
| a) | Le seuil de sécurité minimal tel que fixé par la législation | 141 |
| (i) | Les dispositions de droit commun | 141 |
| (ii) | Les dispositions propres à certaines industries | 144 |
| (iii) | Les limites de la référence aux sources législatives | 148 |
| b) | Le seuil de sécurité maximal tel que fixé par la législation | 150 |

| | |
|--|-----|
| (i) Le difficile équilibre entre accessibilité et confidentialité | 152 |
| (ii) Le difficile équilibre entre sécurité informationnelle et sécurité publique . . . | 162 |
| 2. Les balises jurisprudentielles de l'obligation de sécurité informationnelle | 174 |
| (i) Les recommandations de la Commission d'accès à l'information du Québec | 177 |
| (ii) Les conclusions du Commissariat à la protection de la vie privée du Canada | 180 |
| CONCLUSION | 191 |
| BIBLIOGRAPHIE | 197 |
| TABLE DE LA LÉGISLATION | 225 |
| TABLE DE LA JURISPRUDENCE | 239 |
| INDEX ANALYTIQUE | 247 |