A3. Identifier l'information stratégique à protéger

Tout entreprise dispose d'une quantité d'informations conséquente, qu'elles soient produites en interne ou émanant de tiers (fournisseurs, clients, partenaires financiers, etc.). Elles ne peuvent bien évidemment pas être protégées toutes de la même façon, au risque de paralyser l'activité de l'entreprise. Une analyse précise des risques est donc un préalable indispensable pour identifier les informations qui sont véritablement stratégiques.

ORGANISATIONNEL

En concertation avec l'ensemble des directions de l'établissement :

➤ Collationner l'ensemble des informations détenues ;

➤ Identifier la sensibilité des informations en fonction du préjudice qu'engendreraient leur divulgation, leur perte ou leur destruction pour la vie de l'entreprise (impact faible, moyen, fort – cf. grille *infra*).

Exemples de questionnement

La perte, la destruction ou la divulgation de cette information est-elle de nature à engendrer … :
… un dommage pour l'activité de la structure ou le déroulement d'un projet ?
… un impact financier ou technique ?
… un impact sur le personnel ?
… un impact en matière d'image et de réputation ?
… une incidence sur la confiance des actionnaires ou des banques ?
… une perte de confiance d'un client ou d'un partenaire important ? Etc.

➤ Évaluer l'occurrence de réalisation du risque, tout en appréciant en particulier s'il s'agit de risques humains et/ou techniques.

Exemple de questionnement

Qui, en interne ou en externe, a accès à cette information ?
Les droits d'accès à l'information sont-ils régis (très limités, restreints, libres) ?
Comment cette information est-elle conservée ? Une sauvegarde régulière est-elle prévue ?
L'information doit-elle être transportée sur un support numérique ou autre ?
Comment les échanges d'informations sont-ils opérés ?
Etc.

➤ Agréger les résultats obtenus dans un outil d'analyse, comme par exemple un tableau de criticité.

➤ En fonction du classement obtenu, appliquer des mesures de protection adaptées et établir une politique de gestion de l'information (accès, diffusion, reproduction, archivage, destruction, etc.). Les informations les plus critiques doivent toujours faire l'objet d'une protection renforcée.

➤ Une information identifiée comme stratégique à un moment donné ne le reste pas forcément, ce qui doit pousser à réitérer périodiquement la démarche.

Au-delà de la seule information stratégique à protéger, cette démarche peut s'appliquer pour l'ensemble des informations nécessaires à la bonne continuité de l'activité de l'entreprise en cas de sinistres (incendie, inondation, catastrophe naturelle, etc.).

Exemple de grille de criticité :

			IMPACT				
			Catastrophique	Majeur	Modéré	Mineur	Insignifiant
			5	4	3	2	1
Probabilité d'occurence	Très forte	5					
	Forte	4					
	Moyenne	3					
	Faible	2					
	Très faible	1					

Appréciation des risques au regard des intérêts à protéger :

Rouge : niveau de risque trop élevé. Le risque est présumé trop important et sa maîtrise est problématique. Il convient de réduire le risque à un niveau acceptable, en formulant des propositions de réduction complémentaires tel un plan de protection adaptées qui permet de sortir de la zone rouge, assorti de mesures de gestion de l'information (accès, diffusion, reproduction, archivage, destruction, etc.). Les informations les plus critiques doivent toujours faire l'objet d'une protection renforcée ;

Jaune : niveau de risque élevé. Il convient de réduire le risque à un niveau plus faible ;

Vert : niveau de risque intermédiaire. Les mesures de maîtrise des risques sont jugées acceptables. Une démarche d'amélioration continue reste cependant pertinente en vue d'atteindre, dans des conditions économiquement acceptables, un niveau de risque aussi bas que possible ;

Gris : Niveau de risque moindre.

Pour aller plus loin

Le *Cloud Act* : conséquences en matière de sécurité économique et juridique

La loi américaine du 23 mars 2018, dite « *Cloud Act* », visant à clarifier l'usage des données hébergées par des opérateurs américains hors du territoire des États-Unis en matière judiciaire, soulève des risques quant à la protection des données des entreprises françaises recourant à des fournisseurs de services numériques soumis à la juridiction américaine. Sur réquisition, hors de toute convention d'entraide judiciaire internationale, elle permet aux autorités américaines d'exiger, de la part des hébergeurs et opérateurs du numérique américains la communication des données qu'ils abritent, quel que soit le lieu où ces données sont localisées dans le monde. Cette loi facilite ainsi l'accès des autorités précitées aux données des utilisateurs européens, qu'elles soient ou non dans le *cloud*, sans que ni les utilisateurs concernés ni les autorités compétentes des pays où ils sont établis n'aient à en être informés. Cette loi présente, dès lors, des risques potentiels, à la fois en matière de protection des données personnelles des citoyens européens et de données sensibles des entreprises.

L'entreprise doit prendre en compte ce risque lorsqu'elle fait appel à un fournisseur américain de services de communications électroniques soumis aux obligations du *Cloud Act*.