Sécurité économique : sécurisons nos entreprises et administrations

La révolution numérique et l'interconnexion des hommes, des machines, des objets et des organisations constituent le nouveau moteur de la compétition économique mondiale. Cette « grande transformation » des modes de production, de consommation et de vie placent les données qu'elle produit au cœur des enjeux de nos sociétés. Elle crée de ce fait à la fois des opportunités et de nouvelles menaces que l'on pourrait qualifier « d'augmentées ». Face à cette tectonique des plaques numériques et technologiques, les entreprises sont exposées à une multitude de menaces souvent inédites qui s'hybrident et déstabilisent ou mettent en péril leur activité (innovations disruptives ou « foudroyantes » et bien sûr intrusions, vols ou perte de données sensibles, atteintes à l'image, aux savoir-faire, aux infrastructures informatiques ou à la réputation, « hacking d'influence »).

Dans ce contexte que doivent faire l'Etat et les entreprises pour se protéger et riposter ? Cette problématique a été l'objet le 16 octobre dernier de discussions fort intéressantes lors de la première édition des *Rendez-vous de la sécurité économique* organisée par la DGE (direction générale des entreprises) et le SISSE (service de l'information stratégique et de la sécurité économique) du ministère de l'économie et des finances à Bercy. « Ces Rendez-vous de la sécurité économique » ont été l'occasion de lancer les 26 fiches pratiques intitulées « La sécurité au quotidien ». Trois tables rondes introduites par un message du ministre Bruno le Maire et animées par Ali Laïdi, l'auteur de l'ouvrage « Le droit nouvelle arme de guerre économique » ont permis de dessiner la nouvelle réalité des risques et des menaces et d'esquisser les pistes de la riposte « public-privé ».

La sécurité économique globale : quelles orientations stratégiques ?

Bruno LE MAIRE, ministre de l'économie et des finances, conçoit la sécurité économique s'exprime à travers trois leviers essentiels à savoir la protection des entreprises quelle que soit leur taille contre les cyberattaques explosives depuis quelques années, le filtrage des investissements directs étrangers (IDE) dans des technologies sensibles fabriquées par les entreprises françaises et également la protection des données sensibles, car elles représentent une valeur considérable pour les entreprises. Thomas COURBE, Directeur général des entreprises (DGE) et commissaire à l'information stratégique et à la sécurité économique esquisse le panorama des menaces niveau mondial. Celles-ci sont caractérisées par une réelle intensification de la menace et se manifestent sous trois formes : l'accroissement de la compétition internationale avec une forte intervention des certains États entraînant une perturbation du jeu de la concurrence, l'arrivée des plateformes numériques qui monopolisent le marché du numérique et de certains secteurs et l'usage du droit comme arme économique qui s'intensifie depuis quelques années, en particulier à travers l'application extraterritoriale des lois par la justice américaine, l'objectif final consistant dans la déstabilisation d'entreprises étrangères concurrentes.

Dans ce contexte d'affrontement, la réponse doit-être européenne et bien sûr française en ce qui concerne nos intérêts stratégiques. Thomas Courbe juge qu'au niveau européen, le projet de directive sur le contrôle des IDE est un grand pas pour l'Union européenne. En France, la réponse de l'État s'articule sur trois leviers d'action : d'abord, le renforcement du dispositif de contrôle des IDE, ensuite le développement d'une politique industrielle en s'appuyant sur le socle du Pacte productif 2025 sur les technologies d'avenir et en fin la réforme de l'organisation de la politique de sécurité économique à l'échelle nationale par le renforcement du rôle des Délégués à l'information stratégique et à la sécurité économique (DISSE). François SOULMAGNON, directeur général de l'AFEP (association française des entreprises du privé), insiste sur le risque très important de vulnérabilité que représente la dimension commerciale et technologique généralisée et mondiale de l'activité des entreprises. Il faut à ce niveau trouver un équilibre sur quelles informations communiquer et à qui.
Abordant la problématique sous cet autre angle, Philippe CLERC, expert intelligence économique internationale et prospective à la CCI France, note que la France a désormais formalisé une démarche aboutie en matière de sécurité économique au cœur de la stratégie d'intelligence économique. A partir de l'enquête de la CCI Bretagne, il pointe cependant une faiblesse de la relation public-privé dans la pratique des PME : seule 17% des PME signalent les incidents aux autorités de l'Etat. Face à l'ampleur des menaces, il juge urgent

de déployer une intelligence prospective des risques afin de garder un temps d'avance sur la criminalité numérique, sur les concurrents, les ruptures du marché et les normes internationales. Patrick Martin, vice-président du MEDEF estime qu'il y a deux sources de menaces : la cybercriminalité et la guerre économique notamment à travers l'utilisation des législations étrangères prédatrices. Par exemple certaines PME françaises dans la région de Bretagne renoncent à se positionner sur certains marchés ou à exploiter certains produits par peur de subir des sanctions des lois des lois extraterritoriales américaines. C'est pourquoi le MEDEF a mis en place un comité de souveraineté économique présidé par Laurent GIOVACHINI. Autre exemple, face à l'hyper-concurrence, certains groupes du CAC40 ont renoncé à la cotation en bourse pour ne pas publier des informations sensibles qu'exigent par obligation de transparence, les autorités.

La sécurité des données constitue aujourd'hui une des priorités du ministre Bruno le Maire qui, annonce la création d'un « cloud national stratégique » en France pour protéger les données sensibles des entreprises françaises. OVH et Atos travaillent pour présenter le projet dit « cloud de confiance » d'ici fin décembre 2019. Cette stratégie s'inscrit dans le cadre d'une politique de souveraineté numérique nationale. Il convient aujourd'hui de construire une démarche de sécurité globale, fondée sur l'intelligence des risques dans tous ces aspects, depuis le climat, l'environnement, le terrorisme, la cybercriminalité, l'économie et le sociétal. Nous avons encore trop tendance, note Philippe Clerc à créer la courbe d'aveuglement, c'est-à-dire focalisant nos alertes sur des silos, sur une ou deux activités. C'est pourquoi aussi la coordination des acteurs est fondamentale en matière de sécurité globale. Le rôle du SISSE est de coordonner le renseignement économique (alertes, anticipation) et la sensibilisation à la sécurité économique, avec les DISSE et les entreprises en régions à travers la diffusion des bonnes pratiques notamment des 26 fiches pratiques en sécurité économique disponible sur le site https://sisse.entreprises.gouv.fr.

L'état de la menace et esquisse de solutions

La grande transformation numérique transforme profondément la société. Selon le ministère de l'intérieur, le taux de pénétration de l'Internet en France est de 88% pour une moyenne de 55% au niveau mondial[1]. Cette situation s'accompagne d'une forte progression de la menace liée au numérique. Selon le représentant de la DGSI, les plus grandes menaces viennent des États, des partenaires et des voisins les plus proches. Aujourd'hui le cyber est une des priorités de la DGSI notamment en matière de sensibilisation des entreprises. Les menaces sont également d'origine juridique. Emmanuel LARDEUX,

1 L'état de la menace liée au numérique en 2019 : https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019

Compliance Officer chez Air Liquide, quant à lui identifie quatre familles de données qui rendent vulnérables les grandes entreprises françaises ayant une forte présence mondiale :

- Les données stratégiques : qui peuvent être capturées par les concurrents (technologie et affaires) ;
- Les données personnelles : capturées par la sphère publique en matière de conformité aux réglementations (RGPD). Au de-là de ce besoin de conformité il y a un problème réputation car elles peuvent constituer moyen de déstabilisation de l'entreprise ;
- Les données compromettantes : peuvent être capturées par des autorités étrangères au travers des enquêtes. C'est tout l'objectif du cloud Act qui cherche à capter des données compromettantes dans le cadre d'enquêtes judiciaires dont certaines n'ont rien à voir.
- Les données classifiées : elles peuvent être capturées par des puissances étrangères.

Cette classification des données, permet la mise en place d'une cartographie des risques et d'en obtenir une vision globale des risques encourus par l'entreprise en vue de définir une meilleure stratégie de sécurité des données sensibles. Car la sensibilité des données peut évoluer dans le temps : une donnée est sensible à un instant donné et peut perdre son caractère sensible au fil du temps et inversement, c'est-à-dire gagner en sensibiliser. C'est la raison pour laquelle il est ébauché l'idée de créer un club de confiance réunissant les acteurs économiques publics et privés sur la problématique de sécurité économique.

Selon Samuel Cette, président de la CMPE Occitanie, pour les TPE et PME, le gros défi central de sécurité économique est la problématique des habitudes et de réflexes des collaborateurs. La sécurité économique en milieu TPE et PME se réduit à la cybersécurité notamment la sécurité du système d'information et la résilience c'est-à-dire la mise en place de plan de continuité d'activité. L'accompagnement des TPE-PME, repose sur la sensibilisation du personnel aux bonnes pratiques, la fourniture de recommandations essentielles en matière de sécurité des données sensibles. Le partage de l'information entre les entreprises, les services de l'État comme le SISSE, l'ANSSI et la DGSI est fondamental pour aider à la résolution des problèmes de cyberattaques.

L'État s'organise et coordonne les actions en matière de sécurité économique

En résumé, la sécurité profonde, concept militaire qu'évoque Philippe Clerc (CCI France) permet d'enrichir la démarche car elle incarne une organisation réticulaire à établir jusqu'au plus profond des territoires pour l'analyse et le traitement des menaces. D'où l'intérêt de mobiliser une véritable intelligence organisationnelle. Selon Joffrey Célestin Urbain, chef du SISSE, la sécurité

économique doit être l'affaire de tous. Une étroite coordination est établie entre le SISSE et les DISSE en régions permettant la remontée de problématiques et la mise en place d'actions de sensibilisation des équipes dans l'entreprise. Philippe Clerc mentionne l'urgence du « réarmement des territoires » et le rôle des CCI qui comme en Bretagne coordonnent leur action avec le DISSE régional associé par exemple à l'enquête sur les pratiques et les besoins des PME en matière d'intelligence économique, mais aussi sur le conseil régional. Cette coordination est également portée par les organisations patronales. Le MEDEF a mis en place des référents régionaux se coordonnant avec les DISSE pour des actions plus efficaces (renseignements, alertes, riposte). Les préfets de régions déclinent la stratégie de l'État vers les départements qui à leur tour diffusent au sein des collectivités et des entreprises. Jean-Pierre Larcher, responsable de la cellule Stratégie, prospective et intelligence économique de la région de Normandie souligne le rôle désormais central des collectivités territoriales en matière d'intelligence économique et donc de sécurité économique. Une convention Etat-Région a été signée dans ce sens en 2018. C'est l'exemple de la charte régionale de cybersécurité en Normandie pilotée par le groupe de travail animé par Jean-Pierre Larcher et Philippe Hugo au sein de Région de France. Le vecteur fondamental est le développement d'une culture de sécurité au sein des entreprises dans les territoires parce que leur survie en dépend fortement.

Boubacar DIALLO
Apprenti Intelligence économique & Data
b.diallo@ccifrance.fr
CCI FRANCE