Vol de données : tous les coups sont permis pour piller l’économie française

Vol de données : tous les coups sont permis pour piller l’économie française

Vol d'ordinateur dans des chambres d'hôtel, disparition de brevets dans le Thalys entre Paris et Bruxelles, pénétration d'agents à l'occasion d'une visite, piratage de technologies… Alors qu'une crise endémique tenaille le pays et réveille les appétits les plus féroces, des fleurons de l'économie française font l'objet d'un pillage vertigineux. Animé par un cynique théâtre d'ombres que ne renierait guère John le Carré, il prendrait même depuis vingt ans une forme industrielle. Cet édifiant état des lieux émane d'un rapport choc de la délégation parlementaire au renseignement, composée de parlementaires tous habilités au «secret-défense» et emmenés par le président de la commission des lois à l'Assemblée, le député (PS) Jean-Jacques Urvoas, qui vient d'effectuer une plongée au cœur des services de renseignements et de la sécurité nationale. Ce document de 175 pages, porté à notre connaissance, pointe une «plurivoracité de la prédation économique» liée à une «technicisation de l'espionnage» mais aussi l'«utilisation croissante du vecteur Internet».

Ainsi, l'année dernière, la seule Direction générale de la sécurité intérieure (DGSI) a recensé des «cas d'ingérence», notamment dans le domaine de «la recherche fondamentale, où la culture de la protection est particulièrement faible, mais également dans l'aéronautique et la santé». Dès septembre 2011, les policiers spécialisés de la sous-direction de la protection du patrimoine économique, basée à Levallois-Perret, avaient révélé dans nos colonnes l'existence de près de 5 000 «cas» en quatre ans. Durant cette période, 3 189 entreprises ont été visées. À ce petit jeu, une cohorte de prédateurs occultes pilotée en sous-main par des agences étatiques ou des multinationales s'attaquait à la grande entreprise comme à la plus petite «pépite».

À ce titre, rappelle le rapport de la DPR, «nos principaux partenaires peuvent aussi être nos meilleurs adversaires dans le domaine économique». Sans les citer, les spectres de grandes puissances comme la Chine ou la Russie se profilent entre les lignes. En février dernier, le groupe Safran a été contraint d'épaissir sa cuirasse après des cyberattaques des sites d'une de ses filiales, le motoriste Snecma. «D'une ampleur limitée» et vite décelée, l'intrusion d'origine indéterminée avait conduit les services de sécurité à neutraliser puis retirer une dizaine d'ordinateurs du réseau de l'entreprise. L'Île-de-France, où 144 cas d'ingérence ont été mis au jour en 2013, concentre près de 20 % des attaques. Les secteurs les plus ciblés étant l'aéronautique, l'énergie nucléaire, les télécommunications, l'aérospatiale, la robotique et les machines-outils.

Le droit, un outil de prédation

«Au-delà de cet espionnage industriel dont l'existence est connue, mais dont les méthodes continuent malheureusement de surprendre des entreprises et des administrations insuffisamment armées, il serait naïf d'oublier que les principales ingérences empruntent aujourd'hui des voies légales», précise le rapport, qui brocarde sans détour les États-Unis, lesquels – ce ne sont pas les seuls – utilisent le «droit comme un puissant instrument de prédation». Ainsi, le rapport détaille la redoutable procédure Discovery, fondée sur le principe fondamental de la common law américaine permettant à un «plaignant d'adresser des demandes de pièces au défendeur afin de cibler son action en justice». Or, les demandes s'avèrent bien souvent extraordinairement vastes (d'où leur surnom de fishing expeditions, «parties de pêche») et peuvent procéder d'une volonté de profiter de cette procédure pour se livrer légalement à de l'espionnage économique. Il en est de même pour le deal of justice, qui permet au Department of Justice (DOJ) d'éperonner de grandes entreprises pour infraction aux lois états-uniennes en matière de corruption qui «s'appuie principalement sur le Foreign Corrupt Practices Act de 1977 et sur les lois de sanctions économiques contre des pays (Cuba, Iran, Libye, Soudan, Syrie…)».

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger.

«Dans 90 % des cas, il s'agit d'entreprises étrangères, dont certains grands groupes français, à l'image de la récente affaire impliquant BNP Paribas», souligne le rapport. La banque, accusée de transactions avec des pays sous embargo économique américain, avait accepté le 30 juin, devant un tribunal de New York, deux chefs d'accusation: «falsification de documents commerciaux» et «collusion» avant d'écoper de 6,5 milliards d'euros d'amende. «L'entreprise doit reconnaître sa culpabilité et négocier le montant de l'amende infligée. En contrepartie, le DOJ renonce aux poursuites pour une période de trois ans, période pendant laquelle l'entreprise doit faire preuve d'un comportement exemplaire, note le rapport. Pour prouver sa bonne foi, et là réside le principal problème, elle doit accepter la mise en place d'un moniteur en son sein, moniteur qu'elle choisit mais dont la désignation définitive est soumise à l'approbation des États-Unis. Le moniteur aura accès à l'intégralité des informations de l'entreprise afin de rédiger un rapport annuel extrêmement détaillé.»

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger. Ou encore, ce qui n'est pas la moindre affaire, dévoiler les démarches concurrentielles à l'étranger. Or, révèle la délégation parlementaire, les services secrets américains peuvent «solliciter toute information nécessaire, y compris les rapports de monitorat» en invoquant le Foreign Intelligence Surveillance Act. En clair, le droit sert de bélier pour forcer la protection et les espions passent derrière pour siphonner le savoir-faire français. Selon nos informations, un grand groupe énergétique français et un tycoon pétrochimique allemand ont récemment subi pareil traitement après avoir versé plusieurs milliards de dollars. Alors qu'aux États-Unis les services secrets et le business entretiennent des relations fusionnelles et souvent consanguines, au point que la CIA a créé et gère le fonds d'investissement In-Q-Tel permettant de capter de précieuses informations concurrentielles. Une source informée confie qu'une PME française développant un logiciel performant a été «tamponnée», sans succès, par cette structure qui lui proposait d'entrer dans son capital.

Proposition de loi sur le secret des affaires

Parmi les propositions très concrètes formulées pour défendre le système immunitaire des entreprises françaises, la Délégation parlementaire au renseignement suggère de jeter enfin les bases d'un dispositif national protégeant le secret des affaires. Évoquée de façon éparse et fragmentaire dans la charte des droits fondamentaux de l'Union européenne, le Code du commerce ou celui des postes et télécommunications, cette notion «n'a pas d'existence juridique stabilisée ni de définition uniforme», note le rapport. Ainsi, en droit, la définition du vol n'intègre pas les biens immatériels. Et, pour l'heure, le délit de révélation d'un secret de fabrique ne concerne que les seuls salariés de l'entreprise. Face à un arsenal répressif lacunaire, Jean-Jacques Urvoas a donc concocté une proposition de loi, déposée en juillet dernier et présentée mercredi devant le Medef, permettant d'inscrire dans le Code du commerce un titre en neuf articles sur le «secret des affaires». Protégeant le potentiel scientifique et technique, les positions stratégiques, les intérêts commerciaux et financiers ainsi que la capacité concurrentielle des entreprises, cette loi prévoit des sanctions pouvant aller jusqu'à sept ans d'emprisonnement et 750.000 euros d'amendes dès lors que la souveraineté nationale est en jeu.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lefigaro.fr/conjoncture/2014/12/18/20002-20141218ARTFIG00005-espionnage-comment-on-pille-l-economie-francaise.php
par Christophe Cornevin