Les enjeux de l'information grise

INTELLIGENCE ÉCONOMIQUE. *L'accès à des données non-publiques est devenu essentiel. Le point lors d'un séminaire à Neuchâtel.*

MARIE RUMIGNANI

Connaître le rapport financier, l'organigramme ou les futures succursales de ses concurrents: ces éléments constituent une partie infime des informations dites «grises». Oscillant entre l'information «blanche», ouverte et facile d'accès à tous, et celle «noire», interdite et secrète, l'information «grise» compose la matière première de l'intelligence économique. Licite et à haute valeur stratégique, cette information est cependant rare, fragmentée et noyée sous un flot de résultats, qui nécessitent de gros investissements humains et financiers pour la traiter. Et pourtant, «les entreprises exigent ces informations de plus en plus complexes, où il faut élargir au maximum nos zones de contacts et de connaissances», explique Stéphanie Perroud, directrice associée chez Pélissier & Perroud, société consulting dédié à la veille professionnelle.

A l'occasion de la 11e journée franco-suisse en intelligence économique et veille stratégique jeudi dernier à la HEG de Neuchâtel, plus d'une cinquantaine de participants, dirigeants, représentants d'entreprises et du monde ont partagé leurs expériences et techniques pour identifier, collecter et traiter ces informations sensibles, mais aussi de sensibiliser le public à la protection des données économiques et aux risques de fuites, plus ou moins volontaires. En présentant notamment leurs très larges potentiels, les intervenants sont revenus sur le rôle central d'internet et de l'intranet pour toutes activités de veille, en présentant notamment son très large potentiel

FRÉDÉRIC MARTINET. Twitter, Facebook ou Linkedin sont des mines d'informations incontournables pour l'intelligence économiques.

et des solutions pratiques pour améliorer la productivité et les résultats de recherches (changer de proxy pour accéder à des données étrangères, utilisation de mapping pour regrouper l'information, créer des canaux de partage de l'information au sein de l'entreprise). Cependant, «le plus gros danger est ce qu'il y est entre la chaise et le clavier», a commenté Frédéric Martinet, consultant et formateur pour Actulligence consulting. En outre des failles de sécurités, des connexions sur des postes publics ou encore des oublis de clés USB sur des ordinateurs, les réseaux sociaux tels que Twitter, Facebook ou encore LinkedIn sont devenus des mines d'informations incontournables pour l'intelligence économiques. Annette Siegl, responsable benchmark et veille industrielle chez l'équipementier Faurecia, abonde largement dans ce sens. «Il suffit de regarder les profils LinkedIn de stagiaires ou d'ingénieurs de la concurrence, qui détaillent leurs expériences et leurs projets de développement pour impressionner les recruteurs.» Elle raconte d'avoir pu suivre une conversation entre un concurrent et un fournisseur sur Twitter, à la vue de tous, ou de trouver sur Youtube une vidéo de la ligne de production d'un concurrent, tournée par «des apprentis très enthousiastes et trop heureux de montrer leurs lieux de travail». Les changements fréquents d'indexation de Google se révèle aussi être un piège qui peut se révéler fatal pour les entreprises. Dernière en date, les présentations sous Prezi, réalisées avec un compte gratuit, sont maintenant accessibles sur le célèbre moteur de recherche. «Des documents secrets et des présentations confidentielles de clients se sont trouvés du jour au lendemain sur les premières pages. Il était même possible un moment de faire du shopping d'informations sur Dropbox», commente Frédéric Martinet. Et la liste semble s'allonger avec des sites comme Slideshares, Docstoc ou Quora. Les blogs, forums de discussions, commentaires de vidéos Youtube ou encore les sites d'évaluation d'entreprises tels que l'américain Glassdoor ou l'allemand Kununu regorgent eux aussi d'informations susceptibles d'intéresser la concurrence. Le consultant met aussi en garde sur le social engineering, la dernière tendance qui effleure souvent l'illégalité. Le principe consiste à récupérer un maximum de données personnelles, via un faux profil ou en les collectant sur les réseaux sociaux, pour accéder à des informations critiques. «Le mensonge n'est ni un crime, ni un délit, mais il est interdit d'usurper l'identité de quelqu'un d'autre» précise Frédéric Martinet.

Néanmoins, tous s'accordent que l'humain reste très complémentaire au numérique. La recherche d'information dite traditionnelle, sur le terrain, directement auprès des personnes, est encore d'actualité. Par exemple, manger dans les mêmes restaurants que ses concurrents, surprendre une conversation lors d'une pause cigarette, lire des informations sur un écran d'ordinateur voisin dans un train, récupérer des documents dans les poubelles, ou comme ironise Frédéric Martinet, «faire couler le champagne à flot, sans oublier de complimenter». Pour Bruno Migeot, fondateur de 2PIE, une entreprise spécialisée dans la sécurité de l'information, la psychologie se révèle être une arme très efficace pour récupérer des informations, en jouant notamment sur le sentiment de culpabilité, l'obligation morale ou encore l'appât du gain. Bien que parfaitement légaux, certains modes opératoires rompent certains codes éthiques, comme de réaliser des entretiens d'embauches fictifs, contacter les fournisseurs, recourir à des méthodes de filatures ou encore de géolocalisation. «Introduire quelqu'un dans une entreprise est illégal, mais exploiter les informations notamment d'un jeune stagiaire est possible. Tout est une question de nuance, de comment on place son curseur éthique tout en se référant à la légalité « souligne Bruno Migeot.

Responsable du Master en Intelligence Economique et Veille Stratégique à la HEG de Genève, la professeur Hélène Madinier relève ce «besoin constant de professionnaliser le métier, et d'avoir des spécialistes qui vont instaurer une veille concurrentielle au sein même de leurs entreprises».■

Contre la contrefaçon horlogère

Selon Michel Arnoux, responsable du service anti-contrefaçon de la Fédération de l'industrie horlogère suisse (FH), les informations «grises» sont essentielles pour démanteler les réseaux. «Nous devons relier des choses qui n'ont rien à voir ensemble, on doit chercher et se focaliser sur le lien entre eux». Les montres contrefaites présentent certaines caractéristiques semblables (un composant chimique, la peinture, un défaut de marquage) qui permettent de les regrouper sous l'une des 130.000 familles déjà identifiées. Les informations peuvent provenir également du ticket d'expédition, du bon de livraison, voire même la calligraphie retrouvée sur les colis. Un robot va alors recouper les informations, les traiter pour finir par recréer les réseaux. Les enquêtes peuvent se poursuivre à l'étranger, notamment en Chine avec plus d'une dizaine de raids par jour. «Mais nous sommes tributaires de la situation locale, et nous sommes plus ou moins tolérés et libres de nos actions». Selon la FH, 29 millions de fausses montres suisses ont été produites en 2013, pour un chiffre d'affaire représentant plus d'un milliard de francs, soit 5% du chiffre d'affaire total de l'horlogerie suisse. (MR)