Intelligence économique et sécurité de l'information : la fonte du secret et des frontières organisationnelles à l'ère du réchauffement numérique

En tant qu'ensemble de pratiques et de métiers tournés vers la maitrise et la protection par les entreprises des informations qu'elles jugent stratégiques, l'intelligence économique a connu des évolutions majeures à l'ère numérique. Les fuites restent cependant la conséquence de négligences, de malveillances, et de compromis entre sécurité et efficacité. La circulation de l'information est une condition du travail en tant qu'activité coopérative. Les informations stratégiques sont des puzzles constitués de pièces d'informations aisément accessibles pour qui maîtrise une plate-forme de veille, et dispose de temps pour rassembler des informations et les analyser. Les règles du jeu de la protection du secret des affaires ont changé sous l'effet du « réchauffement numérique » et mis en évidence le caractère illusoire des efforts de délimitation de frontières organisationnelles étanches.

L'ère numérique a modifié profondément les entreprises, leur modes d'organisation du travail et leurs interrelations avec leur environnement. Les outils et les pratiques visant la maîtrise de l'information stratégique ont *a fortiori* aussi évolué. L'équivalent français des *business intelligence* et *competitive intelligence studies*, est l'intelligence économique (IE), qui demeure un champ disciplinaire et professionnel ambigu. Les définitions et visions de l'IE sont nombreuses et contradictoires (Martre, 1994, Carayon, 2003, Moinet, 2011, Delbecque et Fayol, 2012, Masson, 2012). L'IE s'intègre bien dans le cadre des théories classiques de l'organisation marquées par les notions d'adaptation à un environnement, de compétition entre entreprises et de rationalisation en interne (Cansell, 2003). La définition retenue ici la décrit comme un ensemble de méthodes et d'actions légales de veille, de management des connaissances, de sécurité et d'influence qui sont orientées vers un double objectif de maîtrise et de protection des informations jugées stratégiques. La sécurité de l'information n'est donc pas la sécurité des systèmes informatiques, ni la sécurité des documents sous leurs formes papier, numériques ou électroniques.

La notion de maîtrise de l'information utilisée par les praticiens (consultant ou enquêteur en IE, veilleur, responsable de la sûreté, gestionnaire des risques informationnels, chargé du management de l'ereputation, lobbyiste, influenceur) est problématique pour les SIC. Elle recouvre des actions pour obtenir davantage d'informations, pour mieux les analyser et les exploiter au cours des processus décisionnels. Elle conjugue les dimensions quantitatives et qualitatives. Or, l'évaluation de la valeur stratégique de l'information est subjective, située et relationnelle. De plus, elle n'est possible qu'*a posteriori*, et risque d'aboutir à des résultats bien différents selon l'échéance et l'instance d'évaluation choisie. Les organisations ne sont pas monolithiques, ni stables, ce qui plaide pour une analyse nuancée des prétentions rationalisatrices de l'IE.

Intrinsèquement liés à la compétition économique et aux stratégies d'entreprise, à travers leur rôle d'analyse du jeu concurrentiel et d'aide à la décision, les spécialistes de l'IE sont réputés travailler au cœur des enjeux du « secret ». Pour autant, les documents et les informations ne sont pas secrets dans l'absolu, le caractère secret procédant d'une relation d'intention de dissimulation et de l'anticipation des préjudices liés à une diffusion. Or, bien avant l'arrivée du numérique, il convenait déjà de ne parler de « secrets » qu'entre guillemets. Tous les secrets dérivent d'une intention de dissimulation bénéficiant d'une portée et d'une durée limitée. À l'ère du numérique et d'Internet, serait-il devenu illusoire de prétendre protéger ses secrets ? Puisque l'on parle de cycle de vie d'un document, quelle peut être l'espérance de vie « se-

crète » d'un document à l'heure des logiciels de veille capables de sonder le « web profond », du web 2.0., des *leaks* et des lanceurs d'alerte ? Dans quelle mesure les technologies utilisées en IE, comme les logiciels de veille, réalisent-elles la promesse effrayante du *panopticon* de Bentham, d'un monde sans aucun hors champ ? Les cabinets de conseil en IE permettent-ils le dévoilement « endoscopique » des activités au sein des organisations ?

D'un point de vue méthodologique, les auteurs ont eu à cœur d'étudier les discours théoriques présents dans les manuels et les enseignements des Masters dont ils sont responsables. Les auteurs sont enseignants-chercheurs en SIC et coresponsables d'un Master d'IE. L'un d'entre eux est aussi directeur d'un cabinet de conseil-formation en gestion de l'information stratégique et concurrentielle. Il observe ainsi de manière privilégiée le renouveau des outils, des savoir-faire et des pratiques d'IE en entreprise. Chaque mission de conseil ou de formation est une occasion d'observation des usages informationnels et communicationnels du secret. Les discours pragmatiques, ceux des professionnels de l'IE, ont été analysés à partir d'une trentaine d'entretiens de recherche dont sont tirés des verbatims cités de manière anonyme. L'enquête intègre une étude de divers écrits de travail et écrits professionnels « marqués » à des fins d'authentification et de sécurisation.

Tout d'abord, nous présenterons l'intelligence économique en tant que secteur d'activités, en évoquant les mythes qui y sont rattachés, son actualité à travers les médias, mais aussi l'évolution des compétences et des outils. Ensuite, nous analyserons le rôle du secret dans les stratégies commerciales et de légitimation de ce secteur d'activité. Puis, nous évoquerons un panel de missions confiées à des consultants en IE qui illustrent la thèse d'une « fonte » toute relative du secret à l'ère numérique.

L'IE à l'ère numérique

Quand la compétition économique fait rage, les entreprises deviennent « informavores » (Libmann, 2011), et elles misent sur les compétences censées leur permettre d'accéder et de faire le tri dans les importants flux d'information accessibles. Elles veulent donc recruter des experts auxquels elles reconnaissent des compétences liées à leur maîtrise des outils techniques de veille et des compétences plus traditionnelles comme la veille sociale ou la capacité d'analyse. Les compétences traditionnelles restent importantes car *« la veille s'est popularisée, les alertes Netvibes, Feedspot et compagnie sont à disposition de tous* ». Les responsables IE-veille-sécurité de l'information sont technophiles et ne valorisent guère leur propre maîtrise des plates-formes de veille : « Chaque outil suppose une prise en main, mais on est accompagné par les prestataires ». Leur discours sur les outils est gourmand :

« Digimind, PowerPoint pour les notes et rapports, InDesign pour la mise en forme des bulletins de veille et une pléthore d'outils gratuits comme les alertes Feedly, Mention, Alerti ainsi que des outils pour surveiller les médias sociaux. J'utilise aussi Mind Manager pour réaliser des mindmaps » ; « J'ai à ma disposition pas mal d'outils, à commencer par des bases de données payantes (actualités, brevets, études de marché), des outils gratuits d'agrégation de news, un logiciel professionnel de veille, une solution AMI, et un logiciel de cartographie professionnel pour mieux analyser les brevets ».

L'ère du numérique a imposé de nombreuses mutations organisationnelles. Tous les salariés ont dû adapter l'organisation de leur travail, leurs pratiques et relations professionnelles face au développement des TIC. Les professionnels de l'information ont *a fortiori* été affectés par la diffusion de nouveaux outils d'enquête, de veille, de diffusion et de protection de l'information. Ils effectuent quotidiennement des activités en lien avec la traçabilité des activités numériques. Nombre d'entre eux, notamment les « juniors », possèdent des compétences en informatique et en ingénierie de l'information qui leur permettent de trier des informations, de les valoriser et de les diffuser, mais aussi de « dénicher » des informations réputées difficilement accessibles.

Le statut des praticiens de l'IE a évolué en même temps que leurs savoir-faire. Ils envisagent la technicité de leur métier comme une réalité surévaluée et dénoncent les « imaginaires leurrant » autour d'outils numériques qui faciliteraient ou se substitueraient au travail humain :

« Un veilleur qui va faire acheter un outil de veille à 100.000 euros par an, c'est-à-dire un outil qui coûte plus cher que lui, ça le dévalorise ! Tu vas expliquer à l'entreprise qu'au final tu n'es qu'un presse-bouton, alors on garde l'outil et on vire la personne ».

Une révolution du secret des affaires ?

Une information confidentielle est selon le lexique de l'Association des professionnels de l'information et la documentation une « information à diffusion restreinte et dont l'accès ou l'usage est explicitement protégé » par une instance (http://www.adbs.fr). La confidentialité et la mise au secret sont donc des constructions qui n'existent que dans le cadre de relations. Elles sont encadrées, réglementées par des instances possédant une autorité coercitive directe ou dérivée : État, ordre professionnel, entreprise. La préservation du secret ou l'obligation de discrétion ne se limitent pas à des professions ayant accès à des informations relevant de la sphère personnelle ou intime : médecins, avocats, banquiers, officiers civils. L'article 226-13 du Code pénal prévoit en effet que « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie ».

Dans la lignée de la législation américaine qui tend à sanctionner l'acquisition, l'appropriation, la divulgation, ou l'usage de secrets d'affaires (Cohen Act, 1996), la proposition de loi de Bernard Carayon sur la violation du secret des affaires destinée selon son auteur « à prévenir, dissuader ou sanctionner le pillage de nos entreprises, destructeur d'emplois » a été votée par l'Assemblée nationale, mais elle reste bloquée devant le Sénat. L'obligation générale de discrétion est une première protection, mais la plupart des contrats de travail incluent une clause de confidentialité. Dans le système juridique français, la protection de l'information est surtout contractuelle et jurisprudentielle. La jurisprudence indique clairement que le salarié peut être sanctionné pour la diffusion d'informations dont l'entreprise prouvera au juge *a posteriori* qu'elles devaient rester « confidentielles » puisque leur diffusion a pu remettre en cause la pérennité de l'entreprise. Le non-respect d'une clause de confidentialité engage la responsabilité civile. Un salarié fautif risque donc non seulement un licenciement pour faute, mais aussi d'importantes sanctions financières en cas de préjudice avéré et de poursuites. Les clauses de confidentialité dessinent donc implicitement un périmètre autorisé de diffusion des informations.

En second lieu, la sécurité de l'information est inscrite dans la matérialité des documents et les signes plastiques, iconiques ou symboliques qui encadrent et prescrivent leur diffusion. Les entreprises acceptent pour fonctionner plus efficacement le risque d'une libre circulation en interne et donc de fuites à l'externe. Chacune définit un niveau acceptable de risque de fuites, car le travail suppose le partage d'informations en confiance. Les entreprises sont donc contraintes d'accepter un compromis entre sécurité et efficacité (Cansell, 2003) et de miser sur la loyauté de leurs salariés. Certains documents se voient assigné un statut spécifique limitant leur circulation interne. L'identification se fait le plus souvent de manière très simple par des consignes ou des mises en garde relatives à l'accès ou à l'usage du document figurant en en-tête ou en filigrane. Des techniques de marquage plus élaborées existent (tampon ou horodateur). Cela dit, des informations stratégiques peuvent être griffonnées sur une feuille de brouillon ou diffusées par email, tandis qu'un marquage attestant de la soi-disant confidentialité d'un document peut constituer une forme subtile de publicité.

La promesse professionnelle de l'IE dans ce cadre est de contribuer à protéger les informations devant rester confidentielles, à sécuriser les activités de travail contre d'éventuelles tentatives illégales d'espionnage industriel, d'améliorer la solidité du mur censé séparer

l'organisation de son environnement. Elle comprend aussi une capacité à faire émerger des informations stratégiques à partir d'un travail d'analyse s'appuyant sur des informations blanches, celles qui peuvent être obtenues rapidement et facilement « *assis derrière son bureau* » : revue de presse, coup de fil, recherche sur Internet par mots-clés sur un moteur de recherche. Les professionnels de l'IE se défendent de s'intéresser aux informations noires qui ne peuvent, selon une norme AFNOR, être acquises que de manière illégale (loi) ou illicite (jurisprudence). Elles relèvent de l'espionnage, pratique dont les professionnels de l'IE se défendent avec d'autant plus de force que leurs métiers souffrent d'une réputation sulfureuse[1].

L'aspect le plus séduisant de cette promesse inclut l'accès à des informations grises dont la définition pose problème comme en témoignent une lecture des sites Internet des cabinets d'intelligence économique et de divers blogs. Deux définitions prêtent à sourire :

« Informations diffusées par des canaux plus discrets mais pas secrets, tels que papiers de recherche, travaux de recherche universitaires, imprimés de toutes natures »[2] *; information obtenue « grâce à des indiscrétions ».*

Deux grandes familles de définition se distinguent. Une première famille est simpliste, mais opératoire, car elle retient comme critère principal celui du temps consacré à la recherche : « *Il faudra donc faire un effort pour y accéder (se rendre sur un salon, activer un réseau…)* ». La deuxième famille techniciste insiste sur les logiciels de veille sur Internet. Accéder à l'information grise suppose de « *posséder des outils de veille [logiciels de type AMIsoftware, Digimind, EuropressSNI, iScope, IXXO, KBcrawl, Lexis Nexis, Qwam, Spotter] et de savoir les utiliser* ». Cette définition s'appuie sur l'idée que de nombreuses informations sont accessibles en ligne, mais non indexées par les principaux moteurs de recherche généralistes, et relèvent donc du « web profond » ou « invisible ».

Se défendant d'être des « espions industriels », les consultants en IE ne peuvent – en théorie - révéler de « secrets » obtenus de manière illégale (informations noires). Leur discours sur le secret relève de la promotion commerciale. Il est désormais de bon ton de dénoncer le culte du secret entendu comme tendance à la rétention et au cloisonnement. La rhétorique du secret vient au service d'un argumentaire publicitaire de légitimation d'une profession. Le recherche et le dévoilement sont surévalués dans les pratiques d'IE au détriment d'un autre concept bien moins vendeur, celui d'intelligence : « *Le client peut entendre : je vous dévoile des secrets, mais pas je vous explique ce que vous avez sous les yeux car j'analyse les infos mieux que vous* ».

Fonte et résistance des secrets à l'ère numérique

Le numérique n'a que très marginalement fait fondre le secret car l'accès à l'information pose des problèmes de coût et de tri à l'heure de « l'infobésité ». L'accès au web profond suppose d'acquérir des logiciels ou des accès coûteux à des plates-formes de veille. Les professionnels de l'IE ne considèrent pas que les *leaks* ont révolutionné leurs métiers car ils génèrent des masses d'informations difficiles à traiter, qui supposeraient de « *mettre plein de gens dessus et à plein temps pour des résultats médiocres* ».

Les ressorts des fuites sont restés la négligence et la malveillance. Au chapitre de la négligence, les profils renseignés sur les réseaux sociaux numériques sont des mines d'information d'autant plus riches que des sites comme Linkedin et Viadeo servent des vitrines pour les

[1] La réputation sulfureuse est parfois méritée car des anciens des « services » se recyclent en consultants en IE. De plus, il est courant d'utiliser la sous-traitance afin de contourner certaines contraintes légales. Certaines actions illégales en France sont légales en Grande-Bretagne, et certains consultants en IE sous-traitent des missions qui ne peuvent être menées à bien que par des détectives privés.

[2] Difficile de ne pas ironiser sur cette définition qui présente le consultant en IE comme un vulgarisateur de travaux de recherche dont le lecteur sait que l'accessibilité est une condition de leur qualité à travers les notions de concurrence et de coopération.

« egos 2.0. » (Lardellier, Bryon-Portet, 2010). Il n'est donc pas rare de pouvoir y lire des informations en apparence anodines, mais qui peuvent devenir des pièces-clés dans la réalisation de puzzles informationnels : nombre de personnes travaillant sous la responsabilité de telle personne, nature et noms des projets dirigés, voire même l'intitulé précis d'une fonction. Les réseaux sociaux professionnels sont devenus des passages obligés dans des stratégies de recherche d'informations parce qu'ils sont d'abord des espaces de mise en scène et en récit de la professionnalité (Desmoulins, 2014).

Deuxième exemple, une entreprise évoluant dans un secteur d'activité réputé sensible a pu obtenir des informations stratégiques relatives à l'organigramme d'un concurrent américain en s'appuyant sur des données disponibles sur les réseaux sociaux numériques, dans des journaux internes et dans des livrets d'intégration distribués par un sous-traitant européen à ses nouveaux embauchés. Ces livrets étaient accessibles sur le web profond. Si l'enquête a supposé un gros investissement en temps, elle n'a fait appel qu'à des outils de veille gratuits. La pratique du microblogging est elle aussi propice à des fuites par négligence. Des informations relatives à un plan social figuraient sur les blogs de syndicalistes d'une filiale locale d'un grand groupe européen (pertes annuelles, chiffre d'affaires, négociations sur le volume des départs volontaires). Elles ont permis de formuler des hypothèses qui ont été testées pendant des salons professionnels : « *Il suffit de voir comment les gens réagissent quand on lance des ballons d'essai* ». Les seules compétences-clés nécessaires étaient de « se débrouiller » en allemand et de posséder des notions de droit social comparé. L'entreprise commanditaire a pu bénéficier d'un avantage décisif lors de négociations. Les professionnels de l'IE s'accordent pour qu'ils sont forts de leur capacité d'analyse et d'intermédiation mais aussi qu'Internet est favorable aux fuites par négligence notamment du fait de politiques de sécurité de l'information trop souples, et d'une maîtrise tâtonnante des règles et des risques propres à l'écriture pour Internet et à la publication en ligne.

Les lanceurs d'alerte de type wikileaks sont connus pour leur rôle politique et éthique de défense des valeurs du service public, mais certains lanceurs d'alerte s'attaquent à des entreprises privées par intérêt personnel (appât du gain, vengeance). Les salariés eux-mêmes sont le plus souvent à l'origine des alertes à la fraude fiscale. Une étude réalisée par le think tank américain *National Bureau of Economic Research* indiquait, suite à une enquête basée sur 230 cas de fraudes dénoncées entre 1996 et 2004 impliquant des entreprises disposant de plus de 750 millions de dollars d'actifs, que près de 20% des dénonciations provenaient des salariés eux-mêmes, loin devant les journalistes, et les autorités financières (Dyck, Morse, Zingales, 2007). Les professionnels de l'IE témoignent aussi de leur rôle dans des négociations quand « *des salariés font du chantage à la fuite et que les entreprises paient pour éviter le scandale* ». Ce n'est alors pas tant le contenu des fuites qui les préoccupent, mais plutôt leur réputation d'entreprise concernée par des problèmes de sécurité de l'information.

Les exemples les plus surprenants dans lesquels Internet a changé la donne en matière de secret sont liés à l'arrivée de Googlearth. De nombreux sites nucléaires ou militaires sont floutés sur Googlearth, et ce à la demande des États, mais les entreprises du secteur privé ne bénéficient que rarement d'un tel privilège. Une entreprise française a pu anticiper l'arrivée d'un nouveau concurrent sur un secteur d'activité précis après avoir diligenté une enquête en Chine, motivée par les « révélations » involontaires d'un professionnel de l'IE qui avait dressé une simple liste des sites d'un concurrent en les classant en fonction de leur capacité approximative de production déduite à partir d'une mesure de la taille de certains sites industriels visionnés sur googlearth. Cet exemple est intéressant en ce qu'il montre bien le caractère expérimental astucieux des pratiques d'IE, la dimension accidentelle du dévoilement de certains secrets suite à la rencontre d'une information anodine avec une capacité de décryptage qui va ensuite lui conférer un statut nouveau d'information stratégique.

Conclusion : confirmation de la dilution des frontières organisationnelles

Au-delà de la formule métaphorique des frontières de l'organisation et du secret en train de fondre sous l'effet du réchauffement numérique, soit de la chaleur dégagée par la couche matérielle du numérique, par les « machines » (Cotte, 2012), travailler sur le secret permet possède des qualités heuristiques pour l'étude scientifique de la communication des organisations puisqu'elle interroge les frontières de l'organisation et la théorie du document.

Internet a changé la donne en imposant une vision techniciste de l'IE et l'imaginaire-leurrant d'outils pouvant se substituer au travail humain de tri, d'analyse et de valorisation. Internet a aussi modifié les règles du jeu de la médiatisation avec la notion de désintermédiation dans la diffusion des informations. La conscience des risques réputationnels est plus aigüe. L'important n'est pas le contenu des fuites, mais le dévoilement de leur possibilité.

Les directions d'entreprise rêvent de consultants en IE capables de sécuriser leur périmètre informationnel et de pénétrer celui de la concurrence dans le respect de la légalité. Les promesses de l'IE interrogent les frontières de l'organisation. Du fait de la diversité des niveaux d'accréditation en interne des salariés, de la complexité des règles prescrivant la diffusion des documents, des leaks et des lanceurs d'alerte, tracer les frontières de l'organisation parait de plus en plus illusoire.

Bibliographie

Bournois F., Romani P.-J. (2000), *L'intelligence économique et stratégique dans les entreprises françaises*, Economica, 300.

Broise (De la) Patrice, Grosjean Sylvie (dir.) (2010), Dossier « Normes et écriture de l'organisation », *Études de communication*, n°34.

Cansell P. (2003), *Management de l'information et connaissance du marché : développement des pratiques collectives d'intelligence économique et de management de l'information dans une démarche d'adaptation de l'entreprise à son environnement*, thèse de doctorat en SIC, UPEMLV.

Carayon B. (2003), *Intelligence économique, compétitivité et cohésion sociale*, La Documentation française, 173.

Cotte D. (2007), « Espace de travail et logique documentaire », *Études de communication*, n°30, janvier, 25-38.

Delcambre P. (2007), « Pour une théorie de la communication en contexte de travail appuyée sur des théories de l'action et de l'expression », *Communication & Organisation*, vol. 1, n°31, 42-63.

Desmoulins L. (2014), « Le dédoublement numérique des consultants en IE sur Linkedin et Viadeo au service de leur recherche d'informations et légitimité professionnelle », in *Diversification et renouvellement des médiations*, Boustany J., Broudoux, E., Chartron G. (dir.), De Boeck Editions, 98-106.

Dyck A., Morse A., Zingales L. (2007), "Who Blows the Whistle on Corporate Fraud?", NBER Working Paper No. 12882, issued in February 2007.

Groleau C., Mayère A. (2007), « L'articulation technologies – organisations : des pistes pour une approche communicationnelle », *Communication & Organisation*, janvier, n°31, 140-163.

Juillet A., Vuillerme, J.-P. (2011), « L'entreprise face aux fuites d'information », *Problèmes économiques*, La documentation française, août 2011, n°3 – 025, 3-8.

Lardellier P., Bryon-Portet C. (2010), « Ego 2.0. Quelques considérations théoriques sur l'identité et les relations à l'ère des réseaux », *Les Cahiers du numérique*, janvier, vol. 6, 13-34.

Libman A.-M. (2011), « Les professionnels de l'information s'attellent à la (re)construction de leur avenir », *Documentaliste-Sciences de l'Information*, février, vol. 48, 20-21.

Mallowan M. (2011), « L'intelligence économique, un modèle à découvrir? », *Argus*, Volume 39, numéro 2, 20 janvier.

Marcon C., Moinet N. (2011), *L'intelligence économique*, Dunod, 123.

Marzano M., « Présentation. » Opacité du réel et traces de vérité : les enjeux du secret, *Cités*, 2006/2 n° 26, 9-14.

Masson H. (2012), *L'intelligence économique, une histoire française, Genèse, acteurs, politiques*, Vuibert, 328.

Moinet N. (2011), *Intelligence économique : mythes et réalités*, éd. du CNRS, 188.

Nart, R. (2013), « L'espion et ses prothèses », *Médium*, octobre, n°37/38, 75.

Rieder B. (2010), « Pratiques informationnelles et analyse des traces numériques : de la représentation à l'intervention », *Études de communication*, février, n° 35, 91-104.

Sissela Bok (1984), *Secrets: On the Ethics of Concealment and Revelation*, Oxford University Press, 352.