Management Summary

Zwahlen, Fabienne, Marti, Irene, Richter, Marina, Konopatsch, Cathrine & Hostettler, Ueli (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Berne: Université de Berne – Institut de droit pénal et de criminologie.

Contexte

L'espionnage économique est un sujet complexe (voir Fleischer 2016 ; Tsolkas et Wimmer 2013). Ceci du fait que dans la pratique, il n'est pas toujours possible de distinguer espionnage économique et espionnage industriel en raison des liens étroits qui unissent les activités étatiques et privées dans de nombreux domaines. Des chiffres fiables font par ailleurs défaut quant au nombre de cas, aux auteurs et aux dommages effectivement subis, précisément aussi parce que les entreprises concernées éprouvent des difficultés à discerner l'espionnage économique de l'espionnage industriel et d'autres activités criminelles (p. ex. chantage). En outre, l'identification des auteurs et de leurs intentions s'avère souvent complexe, et les attaques passent totalement inaperçues dans de nombreux cas. Parallèlement, une multitude d'entreprises renoncent à signaler les soupçons et les cas d'espionnage concrets par crainte d'une atteinte à leur réputation ou de pertes économiques si de telles informations venaient à être rendues publiques. De fait, le nombre de cas non recensés est vraisemblablement élevé, et les connaissances en matière d'espionnage industriel d'autant plus lacunaires (voir Kaspar 2014 ; Wimmer 2015).

En parallèle d'études réalisées par des sociétés de conseil comme KPMG et PWC (KPMG 2019 ; PWC 2016), une étude scientifique a récemment été menée dans l'espace germanophone par l'Institut Max-Planck de droit pénal étranger et international en collaboration avec l'Institut Fraunhofer de recherche sur les systèmes et les innovations. L'étude WISKOS (Bollhöfer et Jäger 2018) montre qu'une PME allemande sur trois a déjà été victime d'espionnage économique ou d'espionnage industriel par le passé. Pour l'heure, aucune étude de ce type n'est disponible en ce qui concerne la Suisse. Afin de mieux connaître l'ampleur de l'espionnage économique en Suisse, le Service de renseignement de la Confédération (SRC) a chargé l'Institut de droit pénal et de criminologie de l'université de Berne de procéder à une étude sur ce sujet auprès des entreprises. Le but consiste en un relevé détaillé de la situation en la matière, une estimation des impacts financiers et autres dommages, ainsi qu'une appréciation de la qualité de la collaboration entre les entreprises et les autorités. Le SRC s'appuiera en outre sur les résultats de l'étude à des fins de pilotage du contre-espionnage et de développement de son programme de prévention et de sensibilisation Prophylax. Concrètement, cette étude devra permettre d'améliorer la prévention de l'espionnage, notamment par la sensibilisation des milieux de l'industrie et de la recherche en Suisse.

Conception de l'étude et approche méthodologique

L'étude comporte deux volets :

1) une **enquête qualitative** auprès des décideurs compétents sur la base d'entretiens individuels ;
2) une **enquête quantitative** dans le cadre d'un contrôle par sondage représentatif auprès d'entreprises pertinentes de tailles variables et actives dans des domaines divers.

Les outils de collecte des données (guide d'entretien et questionnaire en ligne) ont été développés en collaboration avec le SRC.

Tableau 1 : aperçu des données de l'étude thématique 1 (qualitative)

	Nombre	Nombre de participants/durée des entretiens
Experts	8	8 * 60-90 min.
PME	27	27 * 60-90 min.
Grandes entreprises	13	15 * 60-90 min.
Hautes écoles/instituts de recherche	3	4 * 60-90 min.

Étude «Wirtschaftsspionage in der Schweiz», Université de Berne, 2020

Tableau 2 : aperçu des données de l'étude thématique 2 (quantitative)

	Nombre	Pourcentage
Contrôles par sondage	**3065**	**100 %**
Retours	**362**	**12 %**
Par secteur économique	Nombre	Pourcentage
Secteur primaire (production de matières premières)	19	5 %
Secteur secondaire (fabrication/traitement des matériaux)	145	40 %
Secteur tertiaire (services)	156	43 %
Pas d'informations	42	12 %
Par taille de l'entreprise	Nombre	Pourcentage
Microentreprises : moins de 10 collaborateurs	33	9 %
Petites entreprises : 10 à 49 collaborateurs	250	69 %
Moyennes entreprises : 50 à 249 collaborateurs	62	17 %
Grandes entreprises : plus de 250 collaborateurs	14	4 %
Pas d'informations	3	1 %

Étude «Wirtschaftsspionage in der Schweiz», Université de Berne, 2020

Cas d'espionnage concrets et cas suspectés au sein d'entreprises

15 % des entreprises interrogées dans le cadre de l'étude quantitative ont déclaré avoir déjà été touchées par un cas d'espionnage économique. Les entretiens individuels ont quant à eux révélé qu'**un tiers des entreprises** avaient déjà été **victimes d'espionnage économique** au moins une fois.

Ces incidents ont été identifiés comme relevant de l'espionnage économique par l'entreprise et/ou par le SRC. La taille de l'entreprise n'a toutefois que peu d'importance, puisque l'espionnage économique touche aussi bien les PME que les grandes entreprises. Les résultats de la présente étude montrent que les secteurs suivants sont particulièrement touchés par l'espionnage économique : industrie du bâtiment/construction, information, communication et édition, construction mécanique et industrie, technologie aérospatiale, armement, industrie pharmaceutique et sciences de la vie, électronique et métrologie. Parmi ces secteurs, la construction mécanique et l'industrie (résultat de l'étude quantitative) et l'industrie pharmaceutique et les sciences de la vie (résultat de l'étude qualitative) sont les plus durement touchées par des cas d'espionnage concrets.
Face à un cas d'espionnage, la question du préjudice se pose très vite. Ce dernier est très difficile à chiffrer, aussi bien par les personnes concernées que par des experts extérieurs. Si certaines études fournissent des estimations pour chaque secteur ou pour l'économie et la société du pays (à l'instar de Bitkom 2016 ; PWC 2016), ces chiffres sont peu fiables pour des raisons d'ordre pratique et méthodologique. Il convient donc de les aborder avec prudence. Le préjudice matériel direct est quant à lui plus simple à estimer, car prenant la forme d'un arrêt de production, de la perte d'affaires ou de mesures supplémentaires de lutte contre l'espionnage, notamment en matière d'informatique, de communication, etc. En revanche, l'atteinte à la réputation à long terme lorsque le cas est rendu public est complexe à chiffrer. Une atteinte à la réputation entraîne potentiellement d'importantes pertes matérielles du fait de la perte durable de contrats et de clients. Au cours de notre enquête, 11 % des entreprises ayant décelé un cas d'espionnage ont indiqué que celui-ci avait mis en péril l'existence de l'entreprise : un constat révélateur des répercussions potentiellement graves de l'espionnage économique.

Prévention

Les entreprises interrogées estiment que la prévention à l'interne est beaucoup plus importante que le soutien de spécialistes externes ou d'organismes étatiques. Pour ce faire, elles mettent en œuvre les divers volets de la prévention (aspects structurels et règlements organisationnels, formation et sensibilisation des collaborateurs, mesures dans le domaine de l'informatique et des télécommunications, ainsi que sécurisation physique et technique). Les efforts de prévention sont néanmoins très inégaux entre les entreprises, puisque fortement tributaires de la taille de la structure et donc des ressources disponibles en matière de prévention de l'espionnage. La sensibilisation aux risques liés aux échanges de données et aux communications numériques (comme les e-mails) est notamment très peu développée au sein des PME.

Futurs développements

Les entreprises interrogées mentionnent en particulier la numérisation et la mondialisation en relation avec les futurs développements. La numérisation crée de nouveaux défis pour les entreprises en matière de gestion sécurisée des données sous forme numérique (données de production, mais aussi données clients). Si un grand nombre d'attaques passent d'ores et déjà par la voie numérique, il convient de s'attendre à une multiplication des intrusions de ce type à l'avenir. La mondialisation représente elle aussi un défi. Les marchés prennent une dimension mondiale, soulevant de nouvelles questions en matière de protection des brevets à l'échelle internationale. Dans le même temps, les partenaires commerciaux, les fournisseurs et la clientèle se répartissent dans le monde entier, alors que chaque pays continue de disposer de son propre contexte juridique et de sa propre culture des affaires. Enfin, les collaborateurs viennent d'horizons de plus en plus lointains, de sorte que les entreprises dont la stratégie consistait à recruter essentiellement des collaborateurs sur la base de références qu'elles connaissaient

personnellement sont confrontées à une forte baisse du nombre de candidats qualifiés. Les entreprises, et tout particulièrement les PME, éprouvent donc des difficultés croissantes à assurer la sécurité lors du recrutement de nouveaux collaborateurs. Pour terminer, il convient de s'interroger sur la dimension politique de cette problématique, ainsi que sur les missions et les ressources institutionnelles et humaines des organismes fédéraux et cantonaux. Selon les experts que nous avons interrogés, la Suisse dispose de ressources institutionnelles et matérielles en matière de prévention et de lutte contre l'espionnage assez limitées par rapport à d'autres pays.

Bibliographie

Bollhöfer, Esther & Jäger, Angela (2018). Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Band A 8 09/2018. Freiburg i. Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Fleischer, Dirk (2016). Wirtschaftsspionage. Phänomenologie – Erklärungsansätze – Handlungsoptionen. Wiesbaden: Springer.

Kasper, Karsten (2014). Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse. Wiesbaden: Bundeskriminalamt.

KPMG (2019). Wirtschaftskriminalität und was man dagegen tun kann. *Audit Committee News – Risk Management & Compliance*. 66 (Q3 2019): 1–6. https://home.kpmg/content/dam/kpmg/ch/pdf/wirtschaftskriminalitaet-was-man-dagegen-tun-kann-de.pdf [consulté le 16.7.2019].

PWC (2016). Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. https://www.pwc.de/wirtschaftskriminalitaet. [consulté le 16.7.2019].

Tsolkas, Alexander & Wimmer, Friedrich (2013). Wirtschaftsspionage und Intelligence Gathering. Neue Trends der wirtschaftlichen Vorteilsbeschaffung. Wiesbaden: Springer.

Wimmer, Bruce (2015). Business Espionage. Risk, Threats, and Countermeasures. Waltham, MA: Elsevier.