Management Summary

Zwahlen, Fabienne, Marti, Irene, Richter, Marina, Konopatsch, Cathrine & Hostettler, Ueli (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Bern: Università di Berna – Istituto di diritto penale e criminologia.

Situazione iniziale

Lo spionaggio economico è una tematica complessa (cfr. Fleischer 2016; Tsolkas & Wimmer 2013). Da un lato, ciò è dovuto al fatto che nella pratica, a causa delle strette connessioni esistenti in diversi settori tra le attività statali e quelle private, non è sempre possibile operare una chiara distinzione tra spionaggio economico e spionaggio industriale e, dall'altro lato, mancano dati affidabili sul numero di casi, sugli autori di reati e sui danni reali. Questo dipende anche dal fatto che per le imprese interessate è complicato distinguere tra spionaggio economico, spionaggio industriale o altre azioni criminali (ad es. estorsione). Inoltre gli autori e le loro intenzioni sono spesso difficili da individuare e in molti casi gli attacchi passano completamente inosservati. Nel contempo molte imprese sono reticenti nel comunicare eventuali sospetti e casi concreti di spionaggio perché spesso temono danni alla reputazione o perdite economiche se queste informazioni diventano di dominio pubblico. Le cifre dei casi non segnalati sono quindi molto elevate e le conoscenze sullo spionaggio economico sono altrettanto lacunose (cfr. Kaspar 2014; Wimmer 2015).

Oltre a studi di imprese di consulenza come KPMG e PWC (KPMG 2019; PWC 2016), attualmente per l'area germanofona esiste in particolare uno studio scientifico recente svolto congiuntamente dall'Istituto Max Planck per il diritto penale estero e internazionale e dall'Istituto Fraunhofer per la ricerca sui sistemi e sull'innovazione. Lo studio WISKOS (Bollhöfer & Jäger 2018) mostra che, in passato, in Germania una PMI su tre è già stata vittima almeno una volta di spionaggio economico o è stata interessata dallo spionaggio da parte della concorrenza. Attualmente non esistono studi in questo senso per la Svizzera. Al fine di analizzare più approfonditamente l'entità dello spionaggio economico in Svizzera, il Servizio delle attività informative della Confederazione (SIC) ha incaricato l'Istituto di diritto penale e criminologia dell'Università di Berna di eseguire un pertinente studio presso le imprese. Obiettivo dello studio è allestire una panoramica dettagliata della situazione, stimare i danni finanziari e i danni in generale e stabilire la qualità della collaborazione tra imprese e autorità. I risultati forniranno inoltre al SIC informazioni per il coordinamento del controspionaggio e per l'ulteriore sviluppo del programma di prevenzione e sensibilizzazione Prophylax. Concretamente permetteranno di migliorare la protezione contro lo spionaggio, tra l'altro, tramite la sensibilizzazione della piazza industriale e di ricerca svizzera.

Struttura dello studio e metodica

Lo studio si compone di due parti:
1) un'**inchiesta qualitativa** presso i decisori competenti, sulla base di interviste individuali
2) un'**inchiesta quantitativa** nell'ambito di un campione rappresentativo di imprese rilevanti di dimensioni e settori diversi.

Gli strumenti di rilevazione (linee guida per le interviste e questionari online) sono stati messi a punto in collaborazione con il SIC.

Tabella 1: Panoramica dei dati di base, parte 1 dello studio (qualitativa)

	Numero	Numero di partecipanti/durata dei colloqui
Esperti	8	8 * 60-90 min.
PMI	27	27 * 60-90 min.
Grandi imprese	13	15 * 60-90 min.
Università/istituti di ricerca	3	4 * 60-90 min.

Studio «Wirtschaftsspionage in der Schweiz», Università di Berna, 2020

Tabella 2: Panoramica dei dati di base, parte 2 dello studio (quantitativa)

	Numero	Percentuale
Campione	**3065**	**100%**
Partecipazione	**362**	**12%**
In funzione del settore economico	Numero	Percentuale
Primario (estrazione delle materie prime)	19	5%
Secondario (fabbricazione/elaborazione delle materie)	145	40%
Terziario (servizi)	156	43%
Nessuna indicazione	42	12%
In funzione delle dimensioni dell'impresa	Numero	Percentuale
Microimprese: meno di 10 collaboratori	33	9%
Piccole imprese: 10-49 collaboratori	250	69%
Medie imprese: 50-249 collaboratori	62	17%
Grandi imprese: oltre 250 collaboratori	14	4%
Nessuna indicazione	3	1%

Studio «Wirtschaftsspionage in der Schweiz», Università di Berna, 2020

Casi concreti e sospetti di spionaggio nelle imprese

Delle imprese intervistate, nello studio quantitativo il **15 per cento** ha dichiarato di essere stato oggetto di un caso di spionaggio economico. Nell'ambito delle interviste individuali è emerso che **un terzo delle imprese** è già stato **vittima** almeno una volta **di spionaggio economico**. Si tratta di eventi che sono stati identificati come spionaggio economico dalla stessa impresa e/o dal SIC.

Le dimensioni dell'impresa non hanno tuttavia un ruolo essenziale: lo spionaggio economico colpisce sia le PMI sia le grandi imprese. I risultati dello studio mostrano che sono interessati dallo spionaggio economico in particolare i settori seguenti: costruzioni, servizi di informazione e comunicazione nonché attività editoriali, fabbricazione di macchinari e apparecchiature, industria, tecnica aeronautica e spaziale, industria degli armamenti, industria farmaceutica e life science, elettronica e tecnica delle misurazioni. Il settore della fabbricazione di macchinari e apparecchiature e quello dell'industria (risultati dello studio quantitativo) nonché dell'industria farmaceutica e life science (risultati dello studio qualitativo) sono quelli più colpiti da casi concreti di spionaggio economico.
Quando si registra un caso di spionaggio, si pone subito la questione del danno, che, sia per gli interessati sia per gli esperti esterni, può essere quantificato soltanto con grande difficoltà. Alcuni studi effettuano invero queste stime per settori o per l'economia nazionale e la società (ad es. Bitkom 2016; PWC 2016), tuttavia per ragioni pratiche e metodiche sono poco affidabili e quindi devono essere presi con la dovuta cautela. Il danno materiale diretto, come una perdita di produzione, la perdita di una commessa o i costi maggiori per la lotta contro lo spionaggio (ad es. informatica, comunicazione, ecc.), è più semplice da quantificare. Più difficile da quantificare è invece il danno d'immagine a lungo termine quando il caso è reso pubblico. Potenzialmente un danno alla reputazione provoca una grave perdita materiale se a lungo termine si perdono commesse e clienti. Nella nostra inchiesta l'11 per cento delle imprese che ha notato un caso di spionaggio ha ammesso che la propria esistenza è stata messa in pericolo. Questo sottolinea gli effetti potenzialmente gravi dello spionaggio economico.

Prevenzione

Le imprese intervistate ritengono che la prevenzione interna sia molto più importante rispetto al sostegno da parte di specialisti esterni o organi statali. A tale scopo si avvalgono dei diversi settori della prevenzione (aspetti strutturali e regolamentazioni organizzative, formazione e sensibilizzazione dei collaboratori, misure nel settore dell'informatica e delle telecomunicazioni nonché sicurezza fisica e tecnica). L'intensità degli sforzi a livello di prevenzione è tuttavia molto varia e dipende fortemente dalle dimensioni dell'impresa e quindi anche dalle risorse disponibili nel campo della prevenzione contro lo spionaggio. Inoltre, soprattutto nelle PMI, la consapevolezza dei rischi legati allo scambio di dati e alla comunicazione digitale (ad es. e-mail) spesso è molto scarsa.

Sviluppi futuri

Per quanto riguarda gli sviluppi futuri, le imprese intervistate richiamano l'attenzione in particolare sulla digitalizzazione e la globalizzazione. Con la digitalizzazione, per le imprese aumentano le sfide per gestire in modo sicuro i dati digitali (ad es. dati sulla produzione, ma anche sui clienti). Se già oggi un gran numero di attacchi avviene per via digitale, in futuro bisognerà prevedere un ulteriore aumento degli attacchi digitali. Anche la globalizzazione rappresenta una sfida. I mercati diventano sempre più globali ponendo anche nuove problematiche, ad esempio legate alla protezione di brevetti a livello internazionale.
Alla stessa stregua, inoltre, l'assetto dei partner commerciali, dei fornitori e della clientela è sempre più globale e i differenti quadri legislativi nazionali esistenti come pure le diverse culture imprenditoriali continuano a rappresentare una sfida. Non da ultimo è sempre più globale anche la provenienza dei collaboratori. Alcune imprese hanno indicato che la loro strategia consiste nell'assumere in primo luogo persone le cui referenze sono già personalmente ben note, ma dal punto di vista dell'evoluzione in atto ciò rappresenta una premessa oltremodo restrittiva per la selezione di personale qualificato. La garanzia della sicurezza nell'ambito del reclutamento di nuovi collaboratori diventa più

difficile, soprattutto per le PMI. Infine si pone anche la questione dell'importanza politica della tematica e dei compiti nonché della corrispondente dotazione di personale dei servizi federali e cantonali competenti. Rispetto ad altri Paesi, secondo gli esperti da noi intervistati la Svizzera dispone di un dispositivo per la prevenzione e la lotta contro lo spionaggio piuttosto esiguo in termini istituzionali e materiali.

Bibliografia

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 [accesso il 16.7.2019].

PWC (2016). Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. https://www.pwc.de/wirtschaftskriminalitaet. [accesso il 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.