

IL PUNTO

Rassegna Giurisprudenziale

Controlli e indagini nel rapporto di lavoro

Difesa del know-how aziendale

EDIZIONE SPECIALE



L'EDITORIALE

Axerta Roundtable: condivisione di conoscenze



Stefano Xodo - CEO Axerta

Questa edizione speciale de “Il Punto” di Axerta Vi propone, nelle pagine che seguono, una sintesi degli interventi che hanno caratterizzato il primo Axerta Roundtable, tenutosi a Milano nel mese di maggio.

L'evento si è svolto nella forma di 5 tavoli tematici presso i quali gli ospiti si sono liberamente avvicinati su sessioni di mezz'ora ciascuno. Ogni tavolo vedeva la presenza di un eminente avvocato, affiancato da un consulente Axerta esperto della materia trattata.

La formula Roundtable mira a creare un luogo di scambio e condivisione di conoscenze, mediante sessioni formative di breve durata caratterizzate da un numero limitato di partecipanti, che possono interagire liberamente, proporre domande e portare esperienze, conoscersi reciprocamente e creare nuovi legami.

Gli esperti presenti a ciascun tavolo hanno approfondito secondo differenti sfaccettature il filo comune dell'evento, rappresentato dalla “Difesa del know-how aziendale”. La tematica, di stretta attualità e spesso

sottovalutata dai vertici aziendali, vede impegnate svariate expertise nel contrasto ai comportamenti scorretti di dipendenti e terze parti, quali contraffazione, concorrenza sleale, violazioni del diritto d'autore e sottrazioni di proprietà intellettuale.

I feedback estremamente positivi che abbiamo raccolto ci dicono che abbiamo intrapreso un percorso fruttuoso: riteniamo pertanto che questo evento possa rappresentare solo il primo di una lunga serie.

Intendo in questa sede ringraziare ufficialmente i relatori esterni (gli Avvocati Guido Carlo Alleva, Antonio Bana, Carlo Fossati, Michele Franzosi, Licia Garotti e Ottavia Raffaelli) e quelli interni (Eleonora Casarotti, Luca Mandelli, Vincenzo Francese, Marilena Guglielmetti e Stefano Martinazzo), i 50 graditissimi ospiti in sala e tutte le persone che hanno duramente lavorato dietro le quinte per rendere possibile la realizzazione del primo Axerta Roundtable: grazie e arrivederci alla prossima edizione!

IL CONTRIBUTO DEGLI ESPERTI

Indagine difensive e tutela del know-how aziendale.



AVV. GUIDO ALLEVA

Studio legale Alleva & Associati

Guido Carlo Alleva (Milano, 1957) è avvocato penalista del Foro di Milano dai primi anni '80. Formatosi presso l'Università Cattolica, con una precedente esperienza in una università francese, è stato allievo del Prof. Alberto Crespi con cui ha poi collaborato sia in sede accademica che professionale. Ha fondato nel 1994 lo Studio Alleva & Associati con il quale si è dedicato alla attività forense penalistica in particolare nell'ambito del diritto penale dell'economia, della finanza, dell'industria e della Pubblica Amministrazione.

Le indagini difensive servono a dotare la Difesa delle parti private del procedimento penale di strumenti attraverso i quali esercitare un pieno e consapevole diritto alla prova.

In un sistema processuale penale di stampo accusatorio, quale, almeno tendenzialmente, è quello italiano, sono le parti a dover provare i fatti di causa e i poteri di integrazione probatoria del Giudice sono, di regola, solo eventuali ed eccezionali. Ciò, fermo restando che, ovviamente, in linea di principio, l'onere della prova della colpevolezza dell'imputato al di là di ogni ragionevole dubbio grava sulla Pubblica Accusa.

In tale contesto, le indagini difensive cercano di colmare, se pur solo in parte, l'inevitabile divario sul piano dei poteri investigativi tra parti private (imputato e persona offesa in primis) e Pubblico Ministero, il quale a sua volta può avvalersi, tra gli altri soggetti, della Polizia Giudiziaria. Va da sé che, per ovvie ragioni di ordine pubblico e tutela delle libertà individuali, a livello di poteri investigativi non potrà mai esserci assoluta parità tra Accusa e Difesa nel procedimento penale. È, infatti, solo l'Autorità Giudiziaria e/o di Polizia Giudiziaria, a poter chiedere e/o disporre, nei casi e nei modi consentiti dalla Legge, determinate attività di indagine particolarmente delicate, in quanto fortemente invasive di diritti fondamentali dei consociati (a titolo di esempio: intercettazioni telefoniche, perquisizioni o sequestri).

Per le indagini difensive il contesto normativo di riferimento sul piano costituzionale è quello tracciato dall'art. 24, comma 2 Cost. sul diritto di difesa, inviolabile in ogni stato e grado del procedimento, e dall'art. 111, commi 2 e 3 Cost., il quale, in conformità dell'art. 6 C.E.D.U., riconosce il diritto al giusto processo, alla parità

tra le parti e a disporre di tempo e condizioni necessari per preparare la propria difesa.

Il codice di procedura penale disciplina le indagini difensive al Libro V con gli artt. 327 *bis* e 391 *bis* e ss..

L'art. 327 *bis* c.p.p. è norma di portata generale e prevede, in sintesi, che:

- fin dal momento del conferimento dell'incarico professionale, risultante per iscritto, il difensore possa svolgere investigazioni per ricercare e individuare elementi di prova a favore del proprio assistito (comma 1);
- la facoltà del difensore di svolgere indagini difensive può essere esercitata in ogni stato e grado del procedimento e anche ai fini della fase di esecuzione per promuovere un giudizio di revisione (comma 2);
- le attività di indagini difensive possono essere svolte, su incarico del difensore, anche da un sostituto processuale, da investigatori privati autorizzati e, quando sono necessarie specifiche competenze, da consulenti tecnici (comma 3).

Alla previsione di cui al comma 1 dell'art. 327 *bis* c.p.p., secondo cui le indagini difensive possono essere svolte sia prima che dopo il procedimento penale¹, si aggiunge quella di cui all'art. 391 *nonies* c.p.p., il quale prevede la possibilità delle c.d. indagini difensive preventive, per tali intendendosi quelle svolte in vista dell'instaurazione di un eventuale procedimento penale. Si tratta di un'opzione che, ovviamente, può essere utile soprattutto a chi, per una qualsivoglia ragione, tema di poter divenire indagato e/o imputato in un procedimento penale e voglia iniziare da subito ad acquisire elementi di prova a propria difesa, nonché a chi abbia necessità di acquisire elementi di prova al fine di capire se sia stato commesso un reato ai propri danni

¹Vale a dire in ogni stato e grado del procedimento o dopo la conclusione di esso, per la fase di esecuzione o per un'eventuale revisione.

IL CONTRIBUTO DEGLI ESPERTI

e/o meglio circostanziare la querela o la denuncia con cui darà impulso a un procedimento penale.

Le ragioni per cui un'impresa debba o possa ricorrere allo strumento delle indagini difensive, ovviamente sempre a mezzo di difensore, sono molteplici. Per esempio, in qualità di persona offesa di reati contro il suo patrimonio o informatici o ancora di illecita diffusione del know-how aziendale oppure nella veste di ente chiamato nel procedimento penale a rispondere ai sensi del D.Lgs. 231/2001.

Il codice di procedura penale prevede alcune attività di indagine difensive tipiche: assunzione o ricezione di dichiarazioni orali o scritte da persone informate sui fatti (art. 391 *bis*, comm 1 e 2 c.p.p.); richiesta di documentazione alla P.A. (art. 391 *quinquies* c.p.p.); accesso ai luoghi (art. 391 *sexies* c.p.p.); accesso ai luoghi privati o non aperti al pubblico (art. 391 *septies* c.p.p.); consulenza tecnica (art. 327 *bis*, comma 3 e 391 *sexies*, comma 1 c.p.p.), anche per attività irripetibili (art. 391 *decies*, comma 3 c.p.p.).

A fronte di questa tipizzazione, la dottrina non ha mancato di evidenziare la residua possibilità di indagini c.d. atipiche, quali, per esempio, i pedinamenti a opera di investigatori privati autorizzati².

Per quanto riguarda le concrete modalità di svolgimento delle indagini difensive e, in particolare, i limiti che il difensore è chiamato a rispettare in prima battuta, non si possono non citare, oltre alle norme del codice di procedura penale³, le regole del Codice deontologico forense, le Linee guida del Garante della privacy e tutte le norme che, in termini generali, vietano determinate condotte. A tale ultimo proposito, ad avviso di chi scrive, è, infatti, da rifuggire l'idea – potenzialmente foriera di serie

conseguenze, tanto per il patrocinatore quanto per la parte assistita – secondo cui il conferimento di un mandato per indagini difensive al penalista possa “giustificare” attività invasive dei diritti e delle libertà altrui normalmente vietate e, magari, addirittura penalmente sanzionate.

Non di rado, soprattutto quando si tratta di dover tutelare il know-how aziendale, è nei confronti del proprio (ex) lavoratore che l'impresa si trova ad avere la necessità di svolgere accertamenti e controlli. In questi casi si pone spesso il tema di svolgere controlli sugli strumenti informatici in uso all'(ex) lavoratore, primo fra tutti quello sulla corrispondenza dell'eventuale account e-mail nominativo, di regola protetto da password, dell'(ex) dipendente.

Quando si tratta di corrispondenza dell'eventuale account e-mail nominativo dell'(ex) dipendente, il problema fondamentale è il difficile bilanciamento di due interessi contrapposti:

- da un lato, l'esigenza del datore di lavoro di tutelare l'immagine e il patrimonio aziendali rispetto a condotte illecite;
- da altro lato, la dignità e la privacy del lavoratore e dei terzi che con quel lavoratore comunicano e/o hanno comunicato (cfr., a titolo di esempio, art. 8 CEDU e art. 15 Cost).

La giurisprudenza nazionale ed europea, nonché il Garante della Privacy, sono ormai da tempo consolidati nel riconoscere una forte sfera di protezione agli account nominativi aziendali a tutela della dignità e della riservatezza del lavoratore. In sostanza, è stata ormai superata l'idea (fatta propria anche da alcune sentenze penali di merito risalenti alla prima parte degli anni 2000) che, poiché il dominio dell'account e-mail reca il nome dell'azienda e lo strumento viene affidato al singolo per scopi lavorativi, tutte le e-mail siano dell'azienda

² Cfr., per esempio, P. TONINI, *Manuale Breve. Diritto processuale penale*, Milano, 2020, p. 501.

³ Cfr., soprattutto, artt.

391 *bis* e ss. c.p.p.

IL CONTRIBUTO DEGLI ESPERTI

Difendere il know how aziendale nell'ambito del rapporto di lavoro.



AVV. CARLO FOSSATI

*Senior Partner, Studio Ichino
Brugnatelli e Associati*

La nozione di know how aziendale.

I presupposti perché un'informazione sia considerata parte del cd. "know-how aziendale" dal nostro ordinamento giuridico, e sia quindi ritenuta meritevole di tutela, sono tre:

- la "segretezza" intesa come non accessibilità agli «addetti ai lavori»;
- la "novità", nel senso di attribuzione di uno specifico vantaggio competitivo a chi le detiene legittimamente e, infine,
- la cd. "secretazione", intesa come sottoposizione, da parte del suo legittimo titolare, a misure idonee a preservarne la segretezza.

Sotto tale ultimo profilo, quindi, si può ben rilevare che l'ordinamento tutela ciò che già i soggetti - ritenendolo rilevante - hanno in qualche modo protetto, cercando di evitarne la diffusione.

In particolare, si noti che il concetto di secretazione è un concetto «dinamico», in ragione del fatto che le misure adottate per secretare le informazioni devono evolversi a fronte della costante evoluzione delle minacce; pertanto, un ruolo fondamentale riveste la tutela endo-aziendale del know-how.

L'imprenditore non può aspettarsi che l'ordinamento protegga la segretezza di dati che non ha protetto prima lui stesso, aggiornando costantemente i propri meccanismi di protezione in funzione dell'evolversi delle minacce.

La tutela del know how aziendale nel rapporto di lavoro subordinato.

La tutela del know-how aziendale nel rapporto di lavoro può essere di due tipi: giuridica e tecnica. Con riferimento alla tutela giuridica, nei rapporti con il personale dipendente è necessario adottare, in azienda, policy con focus speciale sulla riservatezza e la tutela dei dati, policy sull'utilizzo dei

beni aziendali con specifiche disposizioni in materia di tutela dei segreti aziendali, policy che regolano lo svolgimento della prestazione lavorativa in regime di smart working prevedendo il divieto di svolgere la prestazione lavorativa in luoghi e/o contesti tecnologici inadeguati, in cui può essere messa a repentaglio la segretezza delle informazioni aziendali.

Quanto, invece, alla tutela tecnica, essa impone l'implementazione in azienda di un'idonea strumentazione tecnologica atta a proteggere i dati contro possibili minacce esterne ed interne.

La sorveglianza da remoto.

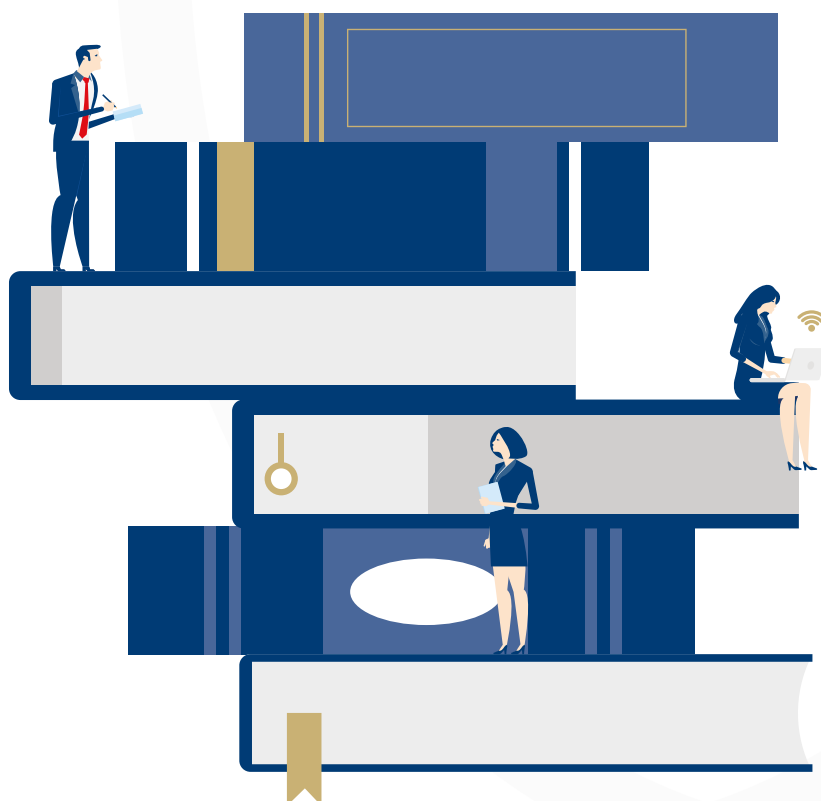
Implementare meccanismi di controllo del personale dipendente, che consentano di prevenire e/o reprimere tempestivamente eventuali violazioni dell'obbligo di riservatezza, significa necessariamente confrontarsi con i limiti imposti, in materia di sorveglianza da remoto, dall'art. 4 dello Statuto dei Lavoratori.

Come noto, l'art. 4 L. 300/1970 opera oggi (dopo le modifiche introdotte con il Jobs Act) una importante distinzione tra strumenti di controllo (comma I) e strumenti di lavoro (comma II): i primi sono essenzialmente gli impianti e gli strumenti audiovisivi dai quali derivi anche la possibilità di controllo a distanza dell'attività lavorativa dei dipendenti: essi potranno venire installati e utilizzati dal datore di lavoro per controllare il personale legittimamente, solo previo accordo sindacale (o, in mancanza, provvedimento autorizzativo dell'ITL) e per le sole finalità organizzative produttive, per la sicurezza sul lavoro, per la tutela del patrimonio aziendale. Gli strumenti di lavoro da cui derivi anche la possibilità, per il datore di lavoro, di effettuare dei controlli da remoto, possono, invece, essere installati senza particolari

IL CONTRIBUTO DEGLI ESPERTI

vincoli, anche in assenza di un accordo sindacale *ad hoc*. Al fine di comprendere meglio la distinzione tra strumenti di controllo e strumenti di lavoro, è intervenuta recentemente la giurisprudenza di merito, definendo lo strumento di lavoro quello concretamente impiegato dal dipendente nello svolgimento delle mansioni distinto dagli strumenti di controllo di cui all'art. 4 comma I, Statuto dei Lavoratori rispetto ai quali il lavoratore è sempre soggetto solamente passivo (Tribunale di Roma 24 Marzo 2017, in *Diritto delle*

Relazioni Industriali, 2018, 1, 264). Infine, diversa dalla fattispecie normativa della sorveglianza da remoto è l'elaborazione giurisprudenziale sui controlli difensivi che travalica i limiti e le condizioni previste dall'art. 4 L. 300/70, ritenendo legittimi i controlli - anche tecnologici - posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti in presenza di una minaccia attuale ovvero del fondato sospetto circa la commissione di un illecito.



La tutela del know-how: prevenzione, segretezza, fedeltà



AVV. ANTONIO BANA
Studio legale Bana

Il delitto di rivelazione di segreti scientifici o commerciali: riforme legislative e casi pratici

Il know-how industriale è una risorsa strategica delle aziende, dalla cui tutela può dipendere la sopravvivenza stessa dell'impresa

Accanto alla protezione offerta in ambito civilistico, il nostro ordinamento offre, grazie anche allo sviluppo della giurisprudenza, protezione in sede penale, in particolare:

- l'art. 623 c.p. («Rivelazione di segreti scientifici o commerciali»);
- l'art. 513 c.p. («Turbata libertà dell'industria o del commercio»);
- D. Lgs. 231/2001 (per il reato di cui all'art. 513 c.p., nonché per i reati c.d. informatici, si può configurare anche la responsabilità amministrativa dell'ente).

Scopo della riforma del 2018

Art.15 , lett.b, l.25/10/2017 (legge delega):

«prevedere misure sanzionatorie penali e amministrative efficaci, proporzionate e dissuasive in caso di acquisizione, utilizzo o divulgazione illecita del know-how e delle informazioni commerciali riservate, in modo da garantire l'efficace adempimento degli obblighi previsti dalla medesima direttiva»

Oggetto del reato

Prima del 2018

(R.D. 19 ottobre 1930, n. 1398)

Rivelazione di segreti scientifici o industriali

1. Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui

profitto, è punito con la reclusione fino a due anni.

2. Il delitto è punibile a querela della persona offesa.

Dopo il 2018

(modificato dal d.lgs. 11 maggio 2018, n. 63)

Rivelazione di segreti scientifici o commerciali

1. Chiunque, venuto a cognizione per ragioni del suo stato o ufficio, o della sua professione o arte, di segreti commerciali o di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, li rivela o li impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni.
2. La stessa pena si applica a chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o altrui profitto.
3. Se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata.
4. Il colpevole è punito a querela della persona offesa.

Dopo la riforma, sono ancora tutelate in sede penale le informazioni riservate ma non segrete ex art. 98 c.p.i., ovvero il «know how in senso lato» (si potrebbe infatti concludere che queste informazioni - asset societario rilevante, non lontano dai segreti, nei contenuti e nel valore - potranno essere protette solo in ambito civilistico ex art. 2598 c.c.)?

Alcune osservazioni:

- tale restrizione dell'oggetto della tutela del segreto in sede penale sarebbe in contraddizione con lo scopo dichiarato del legislatore del 2018 di rafforzare la protezione di tali informazioni;
- l'elemento oggettivo delle

IL CONTRIBUTO DEGLI ESPERTI

fattispecie punite dall'art. 623 c.p. non sembra tuttavia esaurirsi nei segreti commerciali:

- a. il legislatore ha mantenuto al (solo) comma 1 - distinte dai segreti commerciali - le notizie destinate a rimanere segrete su scoperte o invenzioni scientifiche
- b. allo stesso tempo sono state eliminate dal testo le notizie destinate a rimanere segrete sopra le applicazioni industriali, con la precisazione che queste rientrano nell'attuale nozione di segreti commerciali delineata dal c.p.i.

La giurisprudenza più recente: Cass. Pen. Sez. V, 20.09.2018, n.48895

I giudici di legittimità hanno poi esplicitamente affermato che *«non vi è necessaria coincidenza fra la nozione di informazioni segrete aziendali ex art. 98 c.p.i. e le notizie di rilevanza industriale destinate a rimanere segrete ex art. 623 c.p.»*, richiamando a sostegno di tale conclusione:

- a. l'antiorità della norma penale rispetto alla tutela dei segreti introdotta con il codice della proprietà industriale nel 2005;
- b. l'esistenza di un'ulteriore tutela delle informazioni aziendali riservate, ma non segrete, fornita in sede civile dalla disciplina della concorrenza sleale che vieta atti contrari alla correttezza professionale ex art. 2598, n. 3, c.c.;
- c. la competenza del tribunale ordinario, e non delle sezioni specializzate in materia di impresa, a decidere sulla domanda di accertamento di una condotta di concorrenza sleale c.d. non interferente, ovvero consistente nell'acquisizione di informazioni aziendali, processi produttivi ed esperienze tecnico-industriali e commerciali (non segrete), non implicante la contraffazione di privative industriali (inclusi i segreti commerciali), mediante lo storno di dipendenti. [Fattispecie in cui un ex dirigente, al momento delle dimissioni, copiava

senza autorizzazione - e successivamente cancellava in modo irreversibile dal personal computer aziendale - alcuni file contenenti dati riservati del proprio datore di lavoro]

Alcuni suggerimenti in ambito 231/01

- «Due diligence IP» al fine di evidenziare tutti i titoli di privativa industriale presenti nel patrimonio industriale
- Valutazione dell'efficacia ed idoneità delle procedure di protezione e valorizzazione dei propri brevetti o simili titoli di IP e dei propri segni distintivi, con riferimento alle procedure operanti nelle società controllate o partecipate straniere
- Predisposizione di Codice Etico idoneo come linea guida nell'ambito della ricerca innovativa o gestione del patrimonio IP.

In questo ambito si può predisporre un vero e proprio sistema di patto di non concorrenza da porre alla base di accordi c.d. «*Secondment*» attraverso contratti di «*Research and Development*» soprattutto nell'ambito di ricerca di tecnologia e innovazioni industriali.

Quale impatto si viene a creare?

Il soggetto che per ragioni di collaborazione professionale entra in contatto con l'Ente – così conoscendo dei titoli di privativa industriale – dovrà essere vincolato dall'Ente a non divulgarli in alcun modo, né a sfruttarli a suo vantaggio o di terzi.

Importante!

L'elaborazione di misure di sicurezza ad hoc (pratiche e contrattuali) comporta numerosi vantaggi:

Rivendicare l'esistenza di segreti commerciali ex art. 98 c.p.i. (ovviamente quando ci sono i requisiti di segretezza e valore economico previsti) e quindi ottenere tutela in sede civile e penale

Provare l'esistenza della volontà di protezione del detentore

Dimostrare l'esistenza del «beneficio significativo» conferito dai segreti commerciali ai fini del Patent Box

IL CONTRIBUTO DEGLI ESPERTI

Sicurezza informatica per la tutela e lo sviluppo del business



AVV. LICIA GAROTTI

Studio legale Gattai, Minoli, Partners

Cybersecurity e rapporti contrattuali: architettura strategica e back to back

La cultura della sicurezza informatica, di per sé piuttosto recente, è incentrata su una visione prevalentemente “egocentrica” delle organizzazioni. La cybersecurity (o meglio, la sicurezza delle informazioni) in azienda è storicamente – e correttamente – trattata con un approccio risk-based, cioè a dire basato sui rischi gravanti sull’organizzazione in sé considerata al fine di determinare i presidi e le misure idonee alla relativa mitigazione e gestione.

Meno enfasi viene data, invece, al contesto relazionale nel quale è inserita e si muove l’organizzazione, caratterizzato quest’ultimo da relazioni con terze parti, fornitori e clienti. Tali relazioni sono chiaramente idonee a creare altrettanti “point of failure”, con riflessi potenzialmente dirompenti sulla strategia di sicurezza adottata dall’organizzazione. Il contratto è, dunque, lo strumento che dovrà essere maggiormente valorizzato e sviluppato proprio per mitigare e gestire il rischio relazionale.

Se le imprese italiane sono ancora oggi restie a una disciplina contrattualmente puntuale dei diversi rapporti, alcuni interventi normativi e regolamentari hanno contribuito a stimolare una maggiore sensibilità sul punto. Ciò, in particolare, con riferimento alla natura del dato trattato o nell’ambito di settori altamente regolamentati – pensiamo, ad esempio, al richiamo esplicito alle istruzioni in materia di sicurezza che il titolare deve imporre al responsabile del trattamento ai sensi del GDPR; o, ancora, alle disposizioni dell’Autorità Bancaria Europea - EBA e di Banca d’Italia relative ai requisiti contrattuali in caso di outsourcing del sistema informativo bancario.

Siamo, tuttavia, ancora lontani da una

vera e propria cultura della “contrattualistica della sicurezza” al di fuori di contesti limitati o, comunque, settoriali. Sotto questa prospettiva, lo strumento della due diligence preventiva in relazione ai livelli di maturità informatica di potenziali fornitori assume un ruolo di primissimo piano. Essa consente, innanzitutto, di valutare il fornitore non solo sotto il profilo operativo o economico, ma anche sotto quello della sicurezza, contribuendo così a una valutazione più accurata e complessiva degli impatti a medio-lungo termine della potenziale relazione contrattuale. In secondo luogo, una accurata analisi preventiva innesca una dinamica virtuosa, introducendo un ulteriore elemento di competitività tra fornitori, basato sul livello minimo di presidi di sicurezza garantiti. Da ultimo, si tratta di un’attività idonea a dare impulso alla predisposizione di piani per l’innalzamento nel tempo dei livelli di sicurezza garantiti dal fornitore, contribuendo così a una sempre maggiore resilienza del sistema nel suo complesso.

La corretta contrattualizzazione degli aspetti di sicurezza informativa con i propri fornitori è dirimente anche in relazione alla regolamentazione dei rapporti con la clientela. Sotto questo profilo, è chiaramente indispensabile assicurare un elevato livello di coerenza tra misure e presidi garantiti rispetto a quanto contrattualizzato con i propri fornitori, secondo un approccio end-to-end che limiti i rischi di zone “scoperte” e di potenziali fonti di responsabilità per l’organizzazione.

La gestione dell’incidente informatico e l’educazione del capitale umano

L’importanza dell’elemento contrattuale nella gestione della sicurezza si avverte ed è di importanza dirimente

soprattutto nella fase patologica connessa a eventuali incidenti di sicurezza. Sotto questo profilo riveste un ruolo centrale una chiara regolamentazione pattizia di ruoli e responsabilità tra le parti, tanto in tema di gestione dell'incidente e supporto, quanto sotto la prospettiva risarcitoria e assicurativa.

Ciò non vale, ovviamente, di per sé ad escludere il rischio di incidente.

Se le misure e i presidi, sotto il profilo tecnico, organizzativo e contrattuale, rappresentano certamente il "cuore" della gestione del rischio informatico nelle organizzazioni, particolare risalto deve essere dato all'aspetto della formazione del personale. Secondo recenti dati, l'uso improprio delle risorse informatiche da parte dei dipendenti è la causa di quasi la metà degli incidenti di sicurezza subiti dalle imprese.

La formazione non può, tuttavia, essere trattata come un adempimento estemporaneo: l'attività formativa e di sensibilizzazione deve essere debitamente pianificata e documentata, anche per finalità di accountability rispetto ai requisiti normativi applicabili (ad esempio, il GDPR) e deve svolgersi in ottica dinamica, tenendo in debita considerazione sia i mutamenti nel contesto dell'organizzazione (ad esempio, il maggior impiego del lavoro da remoto), sia quelli legati al contesto esterno e ai mutamenti nelle minacce.

La sottrazione e la perdita dei dati riservati di terzi: quale responsabilità per l'impresa?

Una gestione accurata e consapevole di tutti gli aspetti connessi alla gestione della sicurezza delle informazioni sopra richiamati reca evidenti benefici anche sotto il profilo della tutela del patrimonio informativo aziendale, limitando nel contempo i rischi connessi all'illecito trattamento di dati da parte dell'organizzazione.

Ciò, chiaramente, si riflette in maniera altrettanto positiva sulla responsabilità dell'organizzazione in

conseguenza di incidenti di sicurezza informatici, tema estremamente variegato e con aspetti spesso poco considerati. Rilevano anzitutto le conseguenze più "immediate" di un incidente, legate prevalentemente alla continuità operativa dell'organizzazione e agli inevitabili riflessi sotto il profilo della responsabilità contrattuale per ritardi e inadempimenti.

Ciò, tuttavia, non esaurisce il tema del rapporto tra incidenti di sicurezza e responsabilità, che tocca molti altri aspetti. Si pensi, ad esempio, alla responsabilità derivante in caso di sottrazione di informazioni riservate di terzi e detenute dall'organizzazione in forza di specifici accordi di confidenzialità; oppure la responsabilità connessa all'illecito trattamento di dati personali, anche sotto il profilo delle cospicue sanzioni irrogate dall'Autorità di Controllo competente; o infine – aspetto troppo spesso sottovalutato – le conseguenze negative sulla reputazione e l'immagine aziendale, con effetti nel lungo termine addirittura più devastanti rispetto alle conseguenze immediate di natura economica.

È del tutto evidente, in conclusione, che l'accrescimento del livello di maturità informatica aziendale non rappresenta più soltanto un presidio "interno" e reattivo, quanto uno strumento proattivo di competitività dell'impresa sul mercato.

IL CONTRIBUTO DEGLI ESPERTI

Concorrenza sleale e appropriazione indebita del know-how aziendale



**AVV.TI MICHELE FRANZOSI E
OTTAVIA RAFFAELLI**

Studio Legale Rucellai&Raffaelli

I segreti industriali costituiscono un asset immateriale fondamentale per le aziende al fine di competere efficacemente sul mercato.

Tale patrimonio immateriale è in primis tutelato dalla disciplina in materia di proprietà intellettuale, dettata dagli artt. 98 e 99 del Codice della Proprietà Intellettuale (CPI), applicabili a condizione che nel caso concreto sussistano i seguenti requisiti ex lege: la segretezza delle informazioni, il valore economico in quanto segrete e, infine, l'adozione da parte del titolare di misure idonee a prevenirne la divulgazione al pubblico e a preservarne il valore competitivo.

Il difetto di uno di tali requisiti non comporta, tuttavia, la non tutelabilità tout court delle informazioni a fronte di condotte appropriative da parte dei concorrenti. Infatti, secondo l'orientamento della giurisprudenza di legittimità e di merito, le informazioni riservate, pur prive dei requisiti sopra ricordati, possono essere comunque tutelabili alla luce della disciplina normativa repressiva della concorrenza sleale prevista all'art. 2598 c.c. La tutela prevista all'art. 2598 c.c. è, dunque, di natura complementare rispetto a quella di cui agli artt. 98 e 99 CPI e consente all'imprenditore di trovare tutela anche nel caso di sottrazione di informazioni che non beneficiano della protezione assoluta dei segreti aziendali. Ciò alle seguenti condizioni: le informazioni non devono essere generalmente note o, comunque, devono essere destinate a non essere divulgate al di fuori dell'attività aziendale; devono

essere idonee a determinare un vantaggio competitivo in capo a chi le detiene; inoltre, dal punto di vista soggettivo, è richiesta la qualità di imprenditore sia del soggetto attivo, sia del soggetto passivo, nonché la sussistenza di un rapporto di concorrenza tra tali soggetti.

Ciò detto, ai fini di un'efficace prevenzione dell'illecita sottrazione di segreti commerciali, che sia ai sensi degli artt. 98 e 99 CPI ovvero ai sensi della disciplina repressiva della concorrenza sleale, non è possibile prescindere dall'adozione di mirate misure di sicurezza, di natura tanto contrattuale, quanto tecnico organizzative.

In particolare, a livello contrattuale va ricordata la stipula di adeguati accordi di riservatezza con dipendenti, collaboratori o terzi cui l'azienda interagisca, utili non solo a vincolare tali soggetti alla riservatezza responsabilizzandoli, ma anche a dimostrare, occorrendo, che l'azienda aveva adottato misure ragionevoli di tutela. Lo stesso dicasi per l'implementazione di uno specifico regolamento aziendale che detti norme stringenti in materia di utilizzo e salvataggio del



IL CONTRIBUTO DEGLI ESPERTI

patrimonio informativo dell'azienda, nonché di policy che disciplinino l'utilizzo dei device aziendali, e ciò anche rispetto all'attività lavorativa svolta da remoto, che spesso rappresenta l'anello debole dell'apparato di tutela in quanto adottato in regime emergenziale e non adeguatamente regolamentato; si aggiungano la predisposizione di corsi di formazione ed informazione dei dipendenti e collaboratori rispetto all'importanza di preservare il patrimonio del know-how aziendale, l'implementazione di un sistema di monitoraggio e controllo in grado di individuare per tempo attività sospette sul sistema informatico (quali, ad esempio, i download sopra una certa dimensione) e la creazione di un sistema di accesso ai dati differenziato e selettivo in base

alla loro confidenzialità e rilevanza per l'attività di ciascun dipendente e collaboratore; infine, andranno valutate misure di protezione informatica, sia a livello software, come la previsione di password adeguatamente gestite, sia a livello hardware, quali ad esempio la disabilitazione fisica delle porte USB e degli altri accessi ai dispositivi aziendali.

L'adozione di tali misure e l'individuazione del corretto grado di sicurezza andrà valutato caso per caso, tenendo conto della tipologia di attività dell'azienda e delle informazioni che si intende proteggere, ricordando che il parametro legale per svolgere una tale valutazione è l'adozione di misure "ragionevoli" per il mantenimento della loro segretezza.





Axerta S.p.A.
Nord-Ovest: Milano - Piazza Duomo 17
Milano - Piazza Duca D'Aosta 14
Nord-Est: Padova - Piazza Insurrezione 10
Centro-Sud: Roma - Via Giulio Cesare 71

www.axerta.it