ATTI

Convegno
La tutela dei dati all'interno dell'impresa
Le novità del Regolamento UE 2016/679 e della Direttiva UE 2016/943

Roma, 14 giugno 2017
c/o Unindustria Lazio

MASSIMILIANO BONDANINI

Il sistema Confindustria presta particolare attenzione ad alcuni aspetti del diritto d'impresa, tra cui i sistemi di controllo all'interno della struttura aziendale. Confindustria ha come principale obiettivo la rappresentanza degli interessi delle imprese e, a tal fine, collabora con il Garante e con i Ministeri competenti per la stesura di linee guida sia in materia di tutela dei dati che sulla legge 331. Attraverso la *Legal Counsel Community*, che unisce i responsabili degli affari legali all'interno delle imprese, e un help desk dedicato, cerca di guidare le aziende su problematiche specifiche, inclusa la prevenzione del contenzioso, offrendo anche consulenza specifica (legale o in altre materie). In materia tributaria, per Confindustria riveste fondamentale importanza il rapporto con Equitalia e con l'Agenzia delle Entrate mentre, in tema di privacy, risulta cruciale la collaborazione con i Ministeri e con il Garante.
Nell'ambito delle proprie attività, Confindustria ha cercato di convogliare alle imprese il messaggio che anche la tutela dei dati deve essere strutturata sulla base di un sistema di gestione integrato con gli altri sistemi aziendali, quale quello della contabilità. Priorità deve essere assicurata all'*enforcing* e ai controlli successivi, onde misurare la capacità dell'azienda di assicurare l'effettività e l'adeguatezza della *compliance* messa in atto.

MARIA BEATRICE DELI

ICC si pone al servizio delle imprese, degli operatori e dei professionisti in diverse aree, in particolare per le questioni normative e tecnico-giuridiche di portata internazionale. La Commission on Intellectual Property di ICC ha come obiettivo quello di promuovere i diritti di proprietà intellettuale, incoraggiare gli investimenti nell'innovazione e nella creatività e favorire uno sviluppo economico sostenibile. La stessa Commissione di recente ha costituito una *Task Force on Trade Secret Legislation*. Su questi input la Commissione IP di ICC Italia conduce le proprie attività individuando così alcune tematiche su cui concentrare la propria attenzione, tra cui *trade secrets*, *labelling and packaging*, *valuation and monetization of IP assets*. A tal proposito si vorrebbe così avviare una collaborazione con la stessa Unindustria su quelle tematiche che si ritiene di dover esaminare con urgenza nel sistema italiano.

MATTIA DALLA COSTA

LES (Licensing Esecutives Society Italia) si occupa di tematiche legate all'individuazione dell'applicazione del *know-how*, l'individuazione dell'applicazione del perimetro dei *trade secret*. L'organizzazione è attiva non solo a livello italiano ma anche europeo e ha recentemente collaborato con la Commissione Europea, rendicontando in merito allo stato dell'arte nel recepimento della Direttiva UE 2016/943, interagendo direttamente con gli estensori della stessa. Per la prima volta l'Italia svolge un ruolo di pioniere, in quanto agli artt. 98 e 99 del CPI garantisce un'ampia tutela del *trade secret*, diversamente dagli altri Paesi UE. Solo la Svezia, infatti, protegge i *trade secrets* con una disciplina normativa dedicata, mentre in tutti gli altri Paesi dell'Unione Europea si operano dei meri rinvii al diritto penale o ad altre disposizioni.

Il 10 gennaio 2017 la Commissione Europea ha adottato la Comunicazione "*Building a European Data Economy*" evidenziando l'importanza del tema della tutela dei dati, che ha carattere trasversale. In particolare, questa Comunicazione solleva la questione dei *non personal machine generated data,* che attualmente non sono disciplinati specificamente in nessuno degli Stati membri e vengono tutelati come diritti di proprietà intellettuale o come *data bank protection* oppure come *trade secrets*.

Per assicurare un'adeguata tutela dei *trade secrets*, occorrerà agire su tre fronti, ossia: la tutela contrattuale mediante la stesura di contratti ad hoc di *non disclosure* con i vari soggetti coinvolti, il profilo tecnico e la predisposizione di un *best practice program* per la *compliance* rivolto alle imprese.
Un primo riferimento ci è offerto dall'industria militare, che già da anni utilizza protocolli molto precisi, da cui si potrebbe prendere spunto, anche se è evidente che la piccola e media impresa ha bisogno di essere accompagnata in questo processo, non potendo dotarsi di sistemi eccessivamente costosi.

MARCO VENTURELLO

Concordando con quanto premesso dall'Avv. Bondanini, occorre veicolare il messaggio alle imprese che i dati e gli adempimenti sui dati non sono solo "carta", bensì rivestono importanza sotto vari profili. Infatti, quello che da un lato è un adempimento *privacy* - quindi un onore e un costo per l'impresa - dall'altro, sotto il profilo della disciplina dei segreti aziendali, può rappresentare un vantaggio competitivo. Si tratta di due facce della stessa medaglia, per cui gli adempimenti a monte si ritrovano a valle, laddove si agisse in giudizio per tutelare l'impresa.
La tutela dei dati, mediante il regolamento e la direttiva, vanno inquadrati nel più ampio progetto Europa 2020 dell'Unione Europea, che mira ad incentivare le imprese e a investire sull'innovazione, fornendo gli strumenti necessari per proteggere le loro idee. Inoltre, la tutela dei dati rientra in quella che è stata definita "Economia 4.0" per cui sono state previste dei rilevanti vantaggi fiscali, laddove si effettuino investimenti. I dati possono essere personali e non personali. I primi sono sicuramente oggetto di tutela sotto il profilo della cosiddetta *privacy*. Tali dati, che singolarmente non hanno grande rilievo, acquistano valore se aggregati. Ad esempio, una società che organizza convegni sia nel campo del diritto che dell'economia, possiede un *database* di

soggetti interessati al diritto e un *database* di soggetti interessati all'economia; tale insieme di dati presenta al contempo un profilo di tutela *privacy*, ma costituisce anche un segreto commerciale ed è altresì tutelato in quanto banca dati. Questi tre ambiti si sovrappongono: l'impresa dovrà infatti adottare delle misure di protezione dei dati ai fini *privacy*, assumendosene oneri e costi, ma potrà servirsi di tale adempimento per argomentare davanti al tribunale e convincere il giudice a tutelare la banca dati come segreto commerciale.
La Direttiva UE 2016/943 è stata adottata nello stesso giorno in cui negli USA, sotto la Presidenza Obama, è stato approvato il *Defence Trade Secret Act*, dimostrando l'importanza dei segreti aziendali anche a livello internazionale. La direttiva non è stata ancora recepita nel nostro ordinamento , ma l'Italia dispone già di una protezione superiore rispetto alla media europea, in quanto i segreti industriali sono tutelati come diritto di proprietà industriale non titolato. Tuttavia, sotto alcuni aspetti la direttiva appare più innovativa rispetto alla giurisprudenza italiana. Un aspetto su cui l'Italia dovrà adeguarsi alle prescrizioni UE è quello della riservatezza del costo dei procedimenti giudiziari. In tal senso bisognerà chiedere al giudice di accordare misure di protezione specifiche al fine di preservare la riservatezza dei dati che sono stati depositati presso la cancelleria del Tribunale. Un profilo operativo di particolare rilievo per le imprese è quello secondo cui la protezione dei segreti commerciali e delle banche dati non deve essere soggetta a formalità amministrative, per cui non si deve depositare un brevetto o un marchio sobbarcandosene i relativi costi.

Dal punto di vista pratico, la tutela dei dati aziendali, oltre ad avere una funzione di difesa dai concorrenti, protegge anche l'impresa da dipendenti infedeli e *spin-off* scorretti (un'ulteriore normativa che tutela l'impresa in questo tipo di contenzioso sono le regole a tutela della concorrenza sleale). Misure adeguate in questo senso possono essere sia procedure interne che tutele a livello contrattuale – e queste ultime rappresentano lo strumento principale di tutela per i rapporti dell'impresa con figure diverse dai dipendenti.

DAVIDE AJELLO

Per un'azienda multinazionale come Menarini la tutela della privacy riveste particolare importanza e il nuovo regolamento avrà un significativo impatto sui processi e sull'*accountability*. *Accountability* è la parola chiave del regolamento che, innovando rispetto alla precedente normativa, imposta tutto l'impianto legislativo sul principio della responsabilizzazione. Il nuovo regolamento impone al titolare, e quindi all'azienda, una serie di adempimenti e valutazioni da compiere *ex ante* rispetto al trattamento dei dati, affinché tale trattamento sia corretto e siano tutelati i diritti degli interessati. In questo contesto, la figura del *Data Protection Officer* è l'elemento chiave, oltre a rivestire un ruolo innovativo soprattutto nell'ordinamento italiano.

Il Gruppo Articolo 29, deputato a coordinare l'attuazione del regolamento, ha emanato delle Linee Guida che specificano come la tutela della privacy si correli con la normativa dei *trade secrets*. Preliminarmente, è importante sottolineare che l'investimento sulla privacy ritornerà utile all'azienda, non solo per la tutela dei dati personali ma anche per l'eventuale protezione dei segreti industriali che possono essere contenuti e far parte di detti dati personali, in quanto le

stesse misure tecnologiche e organizzative applicate alla tutela dei dati personali sono necessarie per raggiungere il livello di sicurezza richiesto dalla normativa sul *trade secrets*.

È fondamentale che in azienda venga diffusa una cultura proattiva al corretto trattamento del dato e al rispetto di determinate misure di sicurezza, al fine di assicurare una protezione a 360°. Menarini ha già predisposto e diffuso delle linee guida aziendali in materia di *antitrust* e intende agire in modo analogo per la *privacy*, cosicché il dipendente possa capire quali sono i valori in gioco e perché è importante che essi vengano difesi e tutelati dall'azienda.

Venendo nello specifico alla questione del *Data Protection Officer*, il regolamento prevede l'obbligo di nomina indipendentemente dalle dimensioni dell'azienda, per cui questa figura può dover esistere anche in un'impresa piccola, qualora l'attività principale[1] della stessa comporti un monitoraggio su larga scala[2] dei dati personali e/o di dati sensibili. Ovviamente, anche gli enti pubblici sono soggetti all'obbligo di nominare un *Data Protection Officer* secondo quanto previsto dal regolamento. È importante notare che in caso di inottemperanza a questa norma, è prevista una sanzione che va fino al 2% del fatturato totale dell'azienda o fino a 10 milioni di euro.

La nomina obbligatoria deve essere documentata e tracciata per iscritto, quindi le valutazioni sull'opportunità o meno di avere un DPO devono essere verbalizzate all'interno dell'azienda e quest'analisi farà parte della documentazione da produrre in base al principio di *accountability* su discrezione del garante. L'obbligo di nomina di un DPO sussiste non solo per il titolare del trattamento - e quindi per le aziende che sono denominate *data controller* - ma anche per i responsabili del trattamento. Di conseguenza, anche l'azienda che effettui il trattamento di dati personali per conto terzi, qualora ricada nelle attività che prevedano la nomina di un DPO (trattamento su larga scala o trattamento di dati sensibili come *core business*) dovrà nominare un *Data Protection Officer*. L'interrelazione fra normativa *privacy* e normativa sui *trade secrets* impone che anche i sub fornitori dell'azienda debbano adempiere a quest'obbligo, nonché adottare adeguate misure di sicurezza. In questo modo, la catena della fornitura viene validata a monte e assume rilievo in caso di furto di dati, di violazione del *know-how* o di *trade secrets*.

Marco Venturello: L'interrelazione tra le discipline è confermata dal fatto che nella direttiva sui segreti commerciali viene espressamente previsto che si debba effettuare un'opera di armonizzazione e raccordo con la normativa in materia di *privacy*, secondo una visione olistica e armonica. Si specifica inoltre che quest'ultima debba prevalere in caso di conflitto fra le due regolamentazioni.

[1] Il Gruppo Articolo 29 ha ravvisato la sussistenza del requisito "attività principale" laddove il trattamento dei dati rappresenti una componente indiscutibile del business ovvero rientri negli obiettivi sociali di una azienda.

[2] Il Gruppo Articolo 29 ha individuato degli elementi per dare una definizione di "larga scala". Si dovrà pertanto tenere conto del numero dei soggetti coinvolti, del volume dei dati, della durata e delle attività che coinvolgono tali dati, della location geografica ove avviene il trattamento, nonché l'esistenza di attività di monitoraggio o tracciamento sistematico del dato.

Ad esempio, la normativa *privacy* garantisce il diritto d'accesso al soggetto a cui si riferiscono i dati e tale diritto può essere esercitato dall'interessato anche nei confronti delle aziende.[3] Se, consentendo l'accesso ai dati, c'è il rischio di compromettere un segreto industriale, quale valutazione deve essere operata dall'azienda? Sicuramente si tratta di una questione che dovrà essere risolta dal DPO, che deve sviluppare una visione olistica a 360° delle due normative. A livello aziendale, occorrerà superare l'approccio "a compartimenti stagni" a favore di una visione maggiormente integrata e creare, per quanto possibile, momenti di confronto istituzionalizzati attraverso specifiche procedure aziendali.

Oggi la normativa prevede anche il diritto alla portabilità dei dati, per cui il soggetto interessato può richiedere all'azienda che i suoi dati vengano consegnati e gestiti da un altro titolare, concorrente. E' l'esempio classico della *portability* nel settore delle telecomunicazioni, ma che ora viene esteso di fatto all'intero mondo *privacy*, creando potenziali momenti di conflitto, che dovranno essere presi in considerazione.

Le attribuzioni organizzative del DPO, così come definite dal regolamento, richiedono che egli sia autonomo e indipendente e che si dedichi in via primaria all'osservanza del regolamento, occupandosi prevalentemente di *privacy* secondo una visione olistica e sistemica dell'attività di trattamento dati dell'azienda; è possibile che il DPO svolga altre funzioni ma queste non devono essere in conflitto con la sua attività principale. Il DPO non può essere rimosso dal suo incarico o penalizzato per inadempimento dei propri compiti e ricopre una funzione di garanzia dell'adempimento del regolamento all'interno della azienda. Un gruppo multinazionale strutturato può nominare un DPO per l'intero gruppo, purché sia facilmente raggiungibile da ciascun stabilimento - secondo criteri di accessibilità concreta - e sia messo nelle condizioni di poter rispondere nel più breve tempo possibile, ad esempio avvalendosi del supporto di un team di collaboratori. In altri termini, le attribuzioni organizzative del DPO richiedono alle aziende di strutturare la propria organizzazione affinché il DPO possa eseguire i propri compiti.

Il DPO dovrà verosimilmente essere un professionista con un elevatissimo grado di competenza legale e normativa, oltre che un'ottima conoscenza dei sistemi informatici e delle misure di sicurezza adottate dall'azienda; inoltre, dovrà avere una conoscenza specifica del business aziendale, e aderire ad elevati standard deontologici. Per quanto riguarda la *seniority*, questa figura dovrà ricoprire un ruolo dirigenziale, essere in grado di valutare e gestire i rischi, fare formazione, conoscere più lingue straniere, nonché avere familiarità con le lobby e le ispezioni. Per quanto riguarda i criteri di autonomia e indipendenza è importante sottolineare tre aspetti: il DPO dovrà decidere in autonomia come gestire l'adeguamento al regolamento all'interno

[3] Il Gruppo Articolo 29 ha fatto chiarito che il diritto di accesso conferisce all'interessato la facoltà di visionare i propri dati ma non anche le elaborazioni degli stessi – risolvendo a monte il problema di violazione del know-how qualora un gruppo di interessati (eventualmente pagati da un concorrente) facesse congiuntamente richiesta di accesso.

dell'azienda,[4] non potrà essere penalizzato o rimosso dall'incarico in rapporto allo svolgimento delle mansioni affidategli e non dovrà avere conflitti di interesse con eventuali ulteriori ruoli svolti all'interno dell'azienda. In particolare, il DPO non può rivestire, all'interno dell'organizzazione aziendale, un ruolo che comporti la definizione delle finalità o modalità del trattamento dei dati personali. All'interno di un'azienda strutturata, il DPO non può ricoprire già ruoli manageriali di vertice (come ad esempio Amministratore Delegato o Responsabile operativo), ma deve essere una figura nuova e dedicata. Se si intende ricercare tale figura all'interno dell'azienda si potrebbe pensare ad un manager di *compliance*, oppure *compliance* e *antitrust*. Il regolamento prevede peraltro la possibilità di nominare un DPO esterno; tuttavia, si richiedono conoscenze talmente specifiche del business che questa figura risulta essere difficilmente reperibile sul mercato. Il DPO dovrà disporre di risorse gestionali (finanziare e personale) di rilievo all'interno dell'azienda, avere un tempo sufficiente per lo svolgimento dei propri compiti e poter contare su un apporto attivo da parte del Senior Management e su un ampio *endorsement* aziendale. Quanto al compenso del DPO, in America, ad esempio, ammonta a circa 170.000 dollari annui.

Ultimo e forse più significativo aspetto è quello della sinergia tra Responsabile *privacy* e Responsabile protezione dei dati - che potrebbe essere un unico soggetto, salvo eventuali conflitti di interesse che andrebbero valutati caso per caso. I punti di contatto sono numerosi: in primo luogo, la normativa sulla *privacy* contiene una precisa definizione di misure di sicurezza, che risulta utile anche per definire il *know-how* come segreto in quanto tutelato mediante misure di sicurezza; in secondo luogo, la normativa in materia di *data breach* - secondo la quale in caso di violazione dei dati personali l'azienda si deve attivare antro 72 ore con una notifica-; ancora, la normativa sul *trade secret* prevede che in caso di furto dei dati, il soggetto che se ne è illecitamente impadronito sia tenuto a risarcire. Pertanto se, da un lato, l'azienda, a seguito di un *data breach* effettuato con un attacco informatico da parte di un concorrente, dovrà risarcire gli interessati dall'altro, richiederà un risarcimento all'usurpatore in sede giudiziale.

Altre questioni importanti che le aziende dovranno prendere in considerazione sono:

- la valutazione del rischio nel trattamento dei dati, che vale anche per la sicurezza del dato soggetto alla segretezza del *know-how*.
- la definizione di procedure per il controllo della tracciatura del dato: la normativa *privacy* prevede l'esistenza di una catena di fornitori uniti da contratti di *data concession agreement*, che possono essere utili strumenti per imporre degli obblighi di segretezza ai partner commerciali.
- la tracciatura dei partner commerciali, per sapere chi ha un effettivo accesso ai dati aziendali.
- la normativa relativa agli ordini interni, che rileva come misura di sicurezza per la protezione dei dati.

[4] Il DPO non risponde, però, personalmente in caso di inosservanza del Regolamento all'interno dell'azienda, potendo così agire in perfetta autonomia.

GIAMPAOLO DI SANTO

La tematica della protezione dei dati riservati e delle informazioni commerciali e industriali è il cuore della tutela delle aziende in Italia. Il nostro Paese tutela i segreti commerciali e industriali già prima dei TRIPS, mediante l'elastica normativa sulla concorrenza sleale (Art. 1598 n. 3) che dal 1994 disciplina le pratiche commerciali non corrette.[5] Nel 1996 i TRIPS hanno avuto un'intuizione estremamente premiante, introducendo nell'ambito della legge sulle invenzioni l'Art. 6 bis. In Italia, con l'adozione del Codice della Proprietà Industriale, sono stati introdotti sia l'Art. 98 che l'Art. 99 per la tutela dei segreti industriali, recependo l'esigenza dell'industria italiana, fatta soprattutto di piccole aziende con grande cultura dell'informazione riservata a difesa dell'ampio *know-how* aziendale. Non a caso, infatti, nascono nelle aziende dei poli che si occupano della stessa tematica, in quanto la cultura viene tramessa dal dipendente (lecitamente e illecitamente).
In breve, l'Italia ha nella tutela del segreto uno strumento concorrenziale fortissimo anche riguardo ai paesi stranieri. Sebbene la potenzialità di brevettare in Italia sia altissima, non siamo un Paese votato alla brevettazione, in quanto la procedura è costosa ed è esperita quasi esclusivamente dalla grande impresa. Al contrario, è molto diffusa la conoscenza riservata e quindi la necessità di tutela.

Ci sono una serie di informazioni che possono rientrare nella definizione di segreti commerciali, *know-how*, segreti industriali, informazioni confidenziali, e non sempre le definizioni sono sovrapponibili. La tutela esistente ha però un minimo comune denominatore, che è la concorrenza sleale. Questa precisazione è importante perché anche quando non dovessero ricorrere le condizioni necessarie e sufficienti per la tutela del segreto ex art. 98 e 99, si potrebbe procedere facendo leva sulla disciplina della concorrenza sleale ex art. 2598, che impone la correttezza professionale all'imprenditore.

La tematica delle informazioni riservate riveste particolare importanza in questo momento. Si pensi ad esempio al caso di Google e Uber in cui, a detta di Google, Uber sarebbe stata creata attraverso una sorta di *spin-off* di soggetti che avrebbero "rubato" una serie di informazioni riservate.

L'art. 98 del Codice della Proprietà Industriale, che è frutto di successive interpolazioni, di fatto attribuisce al segreto industriale la natura di diritto con una propria autonomia. Pur non trattandosi di un diritto titolato, perché non esiste un registro, esso gode di una specifica tutela. Ciò ha consentito ai giudici di emanare provvedimenti a protezione dei segreti industriali, avvalendosi dei medesimi strumenti di tutela previsti per i brevetti, per i marchi e per tutti gli altri diritti titolati – es. procedimento di descrizione, azione inibitoria, sequestro e provvedimenti cautelari. Va da sé che i segreti industriali o commerciali debbano rispondere ad alcuni requisiti per aspirare a questa tutela.

[5] Il sistema giudiziario italiano in materia di proprietà industriale è di primissimo ordine sia per la competenza dei giudici delle giurisdizioni specializzate, sia per l'efficacia degli strumenti cautelari.

Prima di tutto, costituiscono oggetto di informazione aziendale le esperienze tecnico-aziendali, comprese quelle commerciali. Con il termine "esperienza" si definisce la capacità di un lavoratore o un gruppo di lavoratori di saper fare in modo unico qualche cosa. Non è certamente tutelabile il fatto che il lavoratore possa esercitare il suo diritto costituzionalmente garantito di cambiare datore di lavoro o mestiere, portando con sé le proprie conoscenze, ma tale diritto potrebbe essere limitato mediante patti di non concorrenza.

Tali esperienze devono essere segrete nel loro insieme e nella loro precisa configurazione, quindi non note o facilmente accessibili, in quanto frutto di una specifica elaborazione. Ad esempio, la lista dei clienti di un'impresa può essere tutelata e a tal fine, non può però essere un mero elenco copiato da Pagine Gialle, ma deve trattarsi di un'elencazione frutto di un'elaborazione, in cui vi sono dei dati sulle forniture che vengono normalmente richieste, le abitudini d'acquisto e così via.

Marco Venturello: La lista dei clienti, persone fisiche, ha una doppia rilevanza sia sotto il profilo della privacy, quando si chiede l'autorizzazione al trattamento e quando vengono trattati i dati, sia sotto il profilo di segreto commerciale dell'azienda.

GIAMPAOLO DI SANTO

Sono tutelabili quelle informazioni frutto di una elaborazione che possono essere decodificate e acquisite solo mediante un'opera di c.d. *reverse engineering*. La giurisprudenza giustamente ha rilevato che se il processo di *reverse engineering* è costoso, incerto e difficile, non fa altro che confermare il fatto che quei dati non erano facilmente acquisibili.

Inoltre, per essere tutelabili, le informazioni devono avere un valore economico, termine che non indica un valore di mercato traducibile,[6] bensì un vantaggio concorrenziale. In altri termini, essere in possesso di un'informazione segreta implica avere qualche cosa che gli altri non hanno e quindi avere la capacità di competere su un livello diverso, migliore rispetto ai concorrenti.[7]

Terzo requisito, il più difficile da provare, è che queste informazioni siano sottoposte a misure da ritenersi ragionevolmente adeguate per mantenere il segreto. Laddove si ricorra al giudice,[8] vi è sempre grande dibattito sotto questo profilo, perché chi vanta l'informazione riservata e ritiene di essere stato leso presenterà un quadro nel quale le misure adottate sono sicuramente sufficienti. Di converso, il convenuto riterrà del tutto inadeguate le misure adottate. Ad esempio, se un gruppo di dipendenti lascia una società e crea una sorta di *spin-off* (probabilmente perché c'è un'altra società - magari straniera - che vuole aprire una filiale in Italia e trova utile spingere i dipendenti a lasciare l'attuale luogo di lavoro in tempi brevi), portando con sé una serie di informazioni che potrebbero portare ad un vantaggio concorrenziale.

---

[6] Questa formula, pensata nel 2003, oggi ha un sapore diverso, se pensiamo alla normativa fiscale. Quindi il criterio del valore economico, concepito in questa accezione, può avere una certa rilevanza.

[7] Quando si tratta di presentare una richiesta risarcitoria, si deve far leva sulle ricadute dell'azione illecita, quali l'aver carpito clienti o fette di mercato proprio grazie alle informazioni indebitamente ottenute.

[8] I casi giudiziari in materia di tutela di informazioni riservate è cresciuto in modo esponenziale. Se si ha un brevetto, ad esempio, potrebbe risultare sufficiente una lettera di diffida al presunto contraffattore per fermare il comportamento dannoso ed evitare il giudizio. Così non è invece in materia di segreti aziendali, più difficili da provare.

Davide Ajello: Una delle misure che la *privacy* impone è la segregazione degli accessi, vale a dire che non tutti i dipendenti dell'azienda possono avere accesso a tutti i *database* aziendali e ai dati personali. I sistemi informatici aziendali sono settati sulla base di diritti riservati ai singoli utenti secondo una logica di competenza, per cui soltanto gli addetti e i dipendenti che svolgono un certo tipo di mansioni possono avere accesso a determinati *database*. Questa misura di sicurezza, richiesta dalla normativa *privacy* e prevista a tutela dei dati, può avere ricadute positive nella difesa dell'azienda dai dipendenti che vogliono trafugare segreti aziendali.

GIAMPAOLO DI SANTO

La segregazione e delimitazione delle informazioni rispetto ai soggetti (ad esempio attraverso *password* o *username*) è fondamentale ma può non risultare sufficiente, dato anche il costante evolversi della tecnologia. Infatti, sebbene qualche sentenza degli anni 2000 abbia ritenuto che le *password* potessero essere sufficienti, tale considerazione è oggi superata. Sarebbe consigliabile adottare ulteriori cautele, per esempio diffondere *policy* tra i dipendenti affinché sappiano che certe informazioni o ambiti aziendali sono riservati, oppure dotarsi di sistemi di tracciabilità, che rilevino qualsiasi intrusione nei dati, anche se questo è molto difficile da attuare. Laddove, davanti al giudice, si provi che non solo era stata adottata una misura di prevenzione, ma anche una misura di tracciabilità, la sussistenza del segreto potrebbe senza dubbio ritenersi provata.

Occorre precisare che la giurisprudenza, con molto buon senso, ha sancito che la valutazione dell'adeguatezza delle misure debba essere effettuata ex-ante e non ex-post, tenuto conto anche delle dimensioni e della natura dell'impresa e dell'attività. E' sufficiente provare che l'impresa ha adottato una serie di misure che ragionevolmente potessero impedire l'accesso alle informazioni segrete. Inoltre, non si richiede che tali misure impediscano oggettivamente l'accesso alle informazioni, altrimenti si imporrebbe un onere eccessivo sull'impresa, che dovrebbe dotarsi sempre di sistemi nuovi e all'avanguardia.

Le informazioni che meritano tutela non devono essere brevettabili pur potendo essere idonee alla brevettazione. La scelta cui si trova di fronte l'impresa è rendere pubbliche le informazioni per ottenerne l'esclusiva, oppure non rivelare alcunché e tutelare le informazioni attraverso il *know-how*. Questa questione non riveste però particolare importanza poiché, nella struttura normativa, riveste maggior valore la forma rispetto al contenuto. E' quindi più importante dimostrare che ci si sia adoperati per tenere segrete e riservate le informazioni che dimostrarne il valore intrinseco.

È importante riportare questa ordinanza che cita:

"*deve ritenersi che sussista effettivamente nel caso qui scrutinato un nucleo di informazioni segrete ed esperienze tecnico-industriali sussumibili nella nozione ex art. 98 del C.P.I.. Invero, i dati, le informazioni segrete e le esperienze tecnico-industriali che Società Alfa S.p.A. intende tutelare con l'avvio dell'azione giudiziaria (cautelare e di merito) di cui trattasi integrano effettivamente i requisiti propri delle "informazioni segrete" di cui all'articolo 98 del C.P.I.. Sul punto appare sufficiente osservare come ciò che la parte reclamata intende tutelare è – in primo luogo - l'insieme dei programmi per elaboratore (software), dei files e delle connesse informazioni tecnico - informatiche utili all'ideazione e alla gestione di piattaforme [di telecomunicazioni] dei propri*

clienti-committenti (*"***dati del sistema informatico delle società clienti, protocolli di intervento, memorandum tecnici, informazioni tecnologiche, relazioni, comunicazioni anche di carattere interno, studi, rapporti, schede, tabulati, elenchi clienti, prezziari, roadmaps di nuovi progetti, materiali didattici, slides ed appunti riferibili a riunioni con clienti***"), tutti dati contenuti all'interno dei propri dispositivi aziendali e creati dai propri ex prestatori di lavoro nell'ambito della loro attività lavorativa svolta alle dipendenze della stessa Società Alfa SpA*" Trib. Torino.

I materiali sopra elencati, che fanno riferimento ad occasioni di confronto sul prodotto offerto dalla società, provano che esso era stato "*customizzato*" dal cliente, quindi non generalmente utile ma specificamente utile per quella azienda.

La norma fa poi riferimento al "soggetto che ha il legittimo controllo del detentore", il quale è legittimato ad agire per la tutela. Questa precisazione è particolarmente importante per i gruppi, ove chi deve tutelare il segreto non è necessariamente colui il quale lo ha realizzato. Infatti, all'interno di società di grandi dimensioni, il segreto potrebbe essere trasmesso anche senza formalità e senza un contratto di licenza – salvo che non sia richiesto ai fini fiscali, per necessità di tracciare il flusso delle *royalty*.

Occorre puntualizzare che è molto importante precisare quando un documento, il contenuto di una mail, ecc. è riservato. Tale indicazione potrebbe essere, seppur non bastando, indice della volontà di mantenere segrete le informazioni, considerando il valore delle stesse, e quindi indice della volontà di tutela.

Per quanto riguarda le misure contrattuali a tutela del segreto, vengono in rilievo i patti di non concorrenza e gli accordi di non confidenzialità. Spesso questi accordi prevedono una durata, ma ciò non è corretto, in quanto gli accordi di non concorrenza dovrebbero essere assicurati nel tempo. Per questo motivo, è molto importante inserire in questi accordi una clausola nella quale si specifica che le informazioni riservate - con la precisa indicazione di quali esse siano - sono tutelate *sine dia*, per cui l'altro contraente non potrà utilizzarle liberamente neppure dopo lo spirare del termine contrattuale.

L'art. 99 è lo strumento operativo concesso al titolare di cui all'art. 98 e sancisce che egli "*ha il diritto di vietare ai terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali informazioni ed esperienze, salvo il caso in cui esse siano state conseguite in modo indipendente dal terzo".*

Si noti che il divieto vale per chi acquisisce le informazioni illecitamente e non per colui che dimostri di averle ottenute legittimamente, in modo autonomo e diverso.

Al secondo comma dell'art. 98 si fa riferimento a tutte quelle informazioni che una azienda deve dichiarare per ottenere, ad esempio, l'autorizzazione all'immissione in commercio - in particolare in caso di prodotti chimici e farmaceutici. In questi casi la *disclosure* non fa venir meno tutela del segreto (anche se taluni sostengono che non si tratti di informazioni segrete nel senso stretto della definizione normativa) e, tenendo conto delle peculiarità di quei settori, si dà atto del fatto che la manifestazione di quelle informazioni è necessaria per ottenere autorizzazioni amministrative.

In molti casi queste azioni cominciano con un procedimento di descrizione, che esiste in Italia ma in molti Paesi non è previsto. I giudici spesso concedono le descrizioni *inaudita altera pars*, a seguito della presentazione di un ricorso molto dettagliato, che include molti documenti e relazioni tecniche, e manifesta al giudice la necessità di agire immediatamente. Con il provvedimento del giudice è possibile entrare in una azienda (anche concorrente), con un Ufficiale Giudiziario, e accedere a computer, sistemi produttivi, ecc., nonché interrogare il personale ottenendo la c.d. "prova liquida", strumento fondamentale per difendersi.[9]

Intervento Gennaro d'Andria: Le misure di sicurezza possono essere rafforzate con autonomi obblighi di confidenzialità e riservatezza imposti individualmente al dipendente e sottoscritti specificamente, eventualmente in via informatica.

Risposta Davide Ajello: Queste misure possono essere appropriate per determinate informazioni e per specifiche figure aziendali. Un altro strumento utile potrebbe essere l'adozione di procedure interne e linea guida aziendali che sottolineano l'importanza della confidenzialità dei dati che i dipendenti utilizzano *day by day*. A seconda del livello di confidenzialità e della protezione che si vuole dare al dato si può valutare quale strumento sia più appropriato.

Intervento Roberto Castiglioni: Si nota che la tutela penale è prevista solo in caso di violazione dei segreti industriali e non per illeciti inerenti al trattamento dei dati e alle pratiche commerciali scorrette. C'è quindi una sola norma penale che fa riferimento al *know-how* industriale, che è stata modificata proprio sulla base delle relative esigenze. La disciplina penale sulla *privacy* dà sicuramente la possibilità di farvi rientrare anche alcuni aspetti del segreto industriale. Per quanto riguarda la parte commerciale, tuttavia, non si può operare tale analogia in quanto si tratta di un diritto industriale non titolato. Pertanto l'unica disposizione che consente di proteggere penalmente tutti i diritti industriali è l'art. 517 ter che tutela soltanto i diritti titolati. Su questo aspetto occorrerebbe valutare l'opportunità di un intervento legislativo, soprattutto perché la tutela penale sarebbe di grande rilievo sotto il profilo di ricerca della prova.

Davide Ajello: la ricerca della prova, soprattutto quando in materia di furto di dati da parte di un dipendente infedele, è collegata alle misure preventive che l'azienda ha messo in atto. Se l'azienda ha un fondato sospetto in relazione ad un comportamento illecito di un dipendente non può effettuare liberamente specifiche verifiche all'interno di computer, account aziendali, ecc. salvo che non abbia preventivamente fornito un'adeguata informativa *privacy* o un manuale tecnico al dipendente, pena l'inutilizzabilità del dato come previsto dalla normativa *privacy*.

Mattia Dalla Costa: L'art. 1 comma 3 prevede che la disciplina del segreto industriale non debba limitare la possibilità del dipendente di cambiare datore di lavoro o di utilizzare la sua esperienza e le sue capacità. In sede legislativa, si è discusso moltissimo sull'utilizzo del termine "*experience*" o "*knowledge*", optando per il primo onde evitare di creare il dubbio che con il secondo, che

[9] A differenza del procedimento di descrizione, il sequestro viene difficilmente concesso *audita altera pars*, in quanto il giudice prima convoca le parti.

significa appunto “conoscenza”, si potesse dare adito a difese capziose, consentendo al dipendente fuggiasco di fare riferimento a specifiche conoscenze che aveva acquisito in azienda.

Intervento partecipante: Molte volte si nota che queste azioni illecite sono condotte dagli ex dipendenti piuttosto che dai dipendenti stessi. Mentre per i dipendenti esiste una tutela *ex lege*, essa non si estende agli ex dipendenti. La Cassazione ha così precisato che deve essere analizzata la finalità della condotta e l’utilità della condotta per la nuova azienda.

Giampaolo Di Santo: Questa interpretazione, che si basa sull’esistenza del’*animus nocendi*, è superata in quanto risultava molto complicato individuare in concreto l’esistenza di tale elemento soggettivo. Con la nuova normativa non occorre più indagare l’elemento soggettivo ma soltanto il profilo oggettivo. L’unico dato soggettivo da prendere in considerazione è che la sottrazione non sia avvenuta illecitamente.

In connessione alla violazione della norma sulle informazioni riservate, potrebbe sussistere anche l’ipotesi della concorrenza sleale, ovvero la violazione della normativa sul *copyright*, laddove fossero state sottratte informazioni sui programmi e sui relativi codici sorgente, (tutelati dalla legge sul diritto di autore).

ELIO DE TULLIO

Riportando la discussione sul tema del modello che le imprese vogliono adottare si può sottolineare che i due modelli esistenti, il modello *trade secret based* e il modello *patent based,* non sono alternativi bensì complementari. Le aziende possono anche adottare dei modelli misti, pur tenendo conto dei costi legati al processo di brevettazione e al mantenimento del brevetto, nonché alla tutela di quelle informazioni che, pur essendo rilevanti e segrete per l’impresa, non rivestono il carattere di inventiva richiesto per la brevettazione.

Marco Venturello: Il brevetto diviene cruciale nel caso in cui il prodotto possa essere oggetto di facile riproduzione. In quel caso si deve scegliere se brevettare o non godere di alcuna protezione.

ELIO DE TULLIO

Qualsiasi attività di ricerca e sviluppo, in una prima fase, antecedente al brevetto, costituisce un *trade secret*. Molto probabilmente il modello corretto da adottare prevede, da un lato, una tutela mediante i brevetti e, da un altro, una tutela attraverso i *trade secrets* - anche cercando di sviluppare eventuali complementarietà. La proposta di inserire all’interno dell’azienda un DPO insieme con un *Trade Secret Officer* potrebbe condurre le imprese a creare degli uffici interni per la tutela della proprietà intellettuale che possano governare l’avvio, lo sviluppo e l’implementazione di strategie di tutela a 360°, attraverso i modelli complementari ritenuti di volta in volta più opportuni, considerando i risultati che si vogliono ottenere.

ICC si è occupata molto del tema della tutela dei *trade secrets*. Nella pubblicazione *Trade Secrets: Tools for Innovation and Collaboration* del 2015 vengono analizzati gli strumenti per la tutela dei *trade secrets* e vengono poste le basi per esporre il punto di vista dell’industria rispetto alle

conclusioni adottate sia in seno alla Commissione Europea, con la direttiva, che negli Stati Uniti con il *Trade Secret Act*. In questa pubblicazione si può reperire uno schema molto interessante sulle differenze tra i brevetti e i *trade secret*, analizzando i pro e i contro di ciascun modello.

Sebbene i *trade secrets* oggi abbiano conosciuto un rilancio di tutela che tutto il mondo industriale apprezza, non bisogna dimenticare il valore anche sociale della brevettazione, che è insito nella divulgazione dopo 18 mesi e consente anche il progresso dell'umanità.

Sotto il profilo dei costi, bisogna riconoscere che le spese di brevettazione e di *litigation* spesso creano difficoltà per le aziende nell'adottare un modello esclusivamente *patent based*. È anche vero, però, che lo sviluppo delle procedure e delle misure richieste dalla direttiva sui *trade secrets* non sarà i privo di costi.

Non bisogna peraltro dimenticare che anche una misura di defiscalizzazione come quella del *patent box*, introdotta nel 2015, in sostanza come target il *know-how*, che poteva essere individuato soltanto attraverso l'implementazione di sistemi attraverso i quali i risultati protetti ad attività di ricerca di sviluppo. Di fatto, si tratta sempre di un sistema di *governance* dell'innovazione che passa attraverso misure, procedure, processi interni, documenti da far circolare tra i dipendenti, nonché protocolli e *software* che consentono all'impresa, da un lato, di attaccare e difendersi di volta in volta rispetto alla sottrazione di segreti commerciali e, dall'altro, di definire il danno e il valore economico dei diritti di ricerca e sviluppo e dei diritti di proprietà industriale che su questi si basano - anche nell'ottica di ottenere delle defiscalizzazioni.

Oggi, la *governance* dei dati, delle informazioni segrete e delle innovazioni è fondamentale per le aziende sia che si sfoci in un modello *patent based*, in un modello *trade secrets based* o in un modello misto. La proprietà intellettuale all'interno dell'azienda deve essere concepita sulla base di un modello olistico che prevede la protezione del prodotto e dell'informazione indipendentemente dallo strumento che l'ordinamento offre che può essere il brevetto, il *trade secret* o il marchio. *Extrema ratio* di questo modello è la concorrenza sleale, il minimo comun denominatore tra i vari tipi di tutela.

Marco Venturello: con l'ultima legge di stabilità sono stati introdotti vantaggi fiscali (e.g. *patent box*) a favore delle imprese che investono nell'innovazione. Quindi lo sforzo che viene richiesto per adeguarsi alla normativa sulla privacy e sui *trade secrets* è poi ripagato da agevolazioni fiscali, che fungono da stimolo per le imprese per investire nell'innovazione.

ELIO DE TULLIO

Il panorama normativo è molto positivo per le imprese che vogliono investire su figure professionali interne di alto livello. Anche le PMI che vogliono crescere devono prendere in considerazione la nuova normativa per ottenere un vantaggio competitivo e accedere a finanziamenti.

Nei nuovi progetti Horizon 2020, nel cui ambito sono stati stanziati dall'UE fino a 2 milioni e mezzo di euro per finanziare attività innovative, uno degli aspetti fondamentali è quello della proprietà intellettuale. L'UE non predilige un modello (*patent based* o *trade secret based*) piuttosto che un altro, ma richiede alle imprese di porsi il problema della gestione dell'attività di ricerca e della relativa valorizzazione. L'IP è anche uno degli indici di valutazione delle attività svolte dalle imprese, ossia un parametro che influenza la Commissione Europea nell'assegnazione delle risorse.

L'EUIPO di Alicante a breve pubblicherà degli aggiornamenti in merito allo stato di implementazione della Direttiva sui *trade secrets*, all'armonizzazione delle normative nazionali nei Paesi dell'UE e di essi contano di rispettare i termini di adozione della normativa (l a cui *deadline* è il 2018).