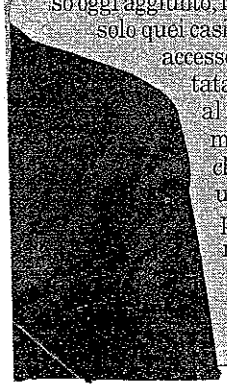
STUDIO GHIDINI, GIRINO & ASSOCIATI

FERRI DEL MESTIERE

Quando l'azienda inciampa sul know how

Come reagireste se un concorrente mettesse le mani sul know how della vostra azienda? Oppure se, più «banalmente» (il virgolettato è d'obbligo), magari con l'aiuto di un dipendente transfuga o, peggio, infedele, venisse trasferita a un concorrente la lista dei clienti di una società finanziaria, completa dei dati relativi alla tipologia di investimenti, alla loro entità e alle varie scadenze contrattuali? Per scongiurare questi rischi esistono norme apposite nel codice civile a tutela della correttezza della concorrenza (art. 2598 n. 3) e, soprattutto, norme più specifiche contenute negli artt. 98 e 99 del codice della proprietà industriale (Cpi). Ma una recente modifica del Cpi (operata dal dlgs n. 131/2010) sembra far scricchiolare il sistema: l'art. 99 è stato infatti riformulato in termini tali da ridurre il perimetro di tutela. Mentre prima (in estrema sintesi) era vietato tout court «acquisire o utilizzare» le informazioni segrete (in cui, per l'appunto, rientra non solo il know how, ma qualsiasi dato aziendale e le esperienze tecnico industriali, comprese quelle commerciali), ora è stato precisato che l'uso, il prelievo e la rivelazione a terzi delle predette informazioni, sono illeciti se perpetrati «in modo abusivo».



Che cosa significa? Sembra che, con l'inciso oggi aggiunto, il legislatore abbia voluto punire solo quei casi in cui v'è stata una modalità di accesso alle informazioni altrui connotata da una condotta scorretta. Ma, al di là delle interpretazioni più o meno sottili della nuova norma, che cosa cambia, in concreto, per un'impresa che voglia tutelare i propri segreti, siano essi le banali liste clienti di cui si è detto o un più complesso know how tecnico? Il cambiamento risiede nel fatto che l'azienda dovrà adottare una certa serie di contromisure per proteggere il bene aziendale fondamentale: piazzare insomma una specie di antifurto sul know how così da rendere sicuramente abusiva la condotta di chi lo violi. Tali contromisure dovranno essere anzitutto di ordine materiale, com'è intuibile. Perciò, tra l'altro, si dovranno proteggere i sistemi informatici in cui sono raccolti i dati con password e altri sistemi. Cautele che però potrebbero non bastare. Perché occorrerà adottare anche appositi antifurti legali che, come rammenta l'art. 98, devono essere «ragionevolmente adeguate» a mantenere il segreto. I sistemi di sicurezza più sofisticati e impenetrabili (Wikileaks insegna!) possono essere più o meno facilmente aggirati specie se si può contare sulla complicità di una quinta colonna. Nell'azienda, poi, il traditore non è solo il dipendente infedele o transfuga, ma qualunque altro soggetto con cui si sia in rapporti: si pensi a un fornitore al quale vengano trasmessi dati riservati nell'ambito della realizzazione di un progetto innovativo. L'azienda deve premunirsi anche nei confronti di queste situazioni rispetto alle quali non c'è password che tenga, ma solo idonei strumenti legali e contrattuali. Un esempio è dato dalla stipulazione di patti di non concorrenza con i dipendenti che impediscano di passare a un concorrente se non dopo un certo periodo dalla fine del rapporto: se non altro, l'eventuale passaggio di informazioni riguarderebbe quelle non più fresche. Quanto ai fornitori, nei contratti non ci si dovrebbe preoccupare soltanto di stabilire prezzi e modalità di pagamento, ma anche il trattamento delle informazioni aziendali segrete, con impegno a non rivelarle, prevedendo penali consistenti: altrimenti, a cose fatte, in sede giudiziaria, sarà molto difficile anche solo recuperare qualche euro di risarcimento. È sorprendente riscontrare quotidianamente come a questo profilo poche imprese prestino la dovuta attenzione, con conseguenze, in pratica, spesso devastanti.

Marco Mergati