PROTEZIONE DEI DATI AZIENDALI E SEGRETO PROFESSIONALE

SOTTOTITOLO

AVVOCATO STEFANO COMELLINI - DOTT.SSA GIULIA ZALI[1]

1. La protezione dei dati aziendali.

Lo sviluppo delle tecnologie informatiche rende sempre più pericolosa, per le imprese, la minaccia che i dati rilevanti per le proprie attività possano essere, anche con mezzi fraudolenti, sottratti ad opera, sia dei propri dipendenti, sia dei soggetti che intervengano professionalmente all'interno dell'azienda o che, comunque, si trovino in una posizione privilegiata di accesso alle informazioni.

Le attività illecite possono consistere, da un lato, nella sottrazione o cancellazione di dati; dall'altro, nell'utilizzo degli stessi, o per avviare un'attività in concorrenza o per rivenderli ad imprese concorrenti.

Riguardo al dipendente, l'obbligo di fedeltà - disciplinato dall'art. 2105 c.c.[2] – consiste nel divieto di concorrenza e nell'obbligo di riservatezza ovvero di segretezza. Il primo consiste nel dovere di astenersi dal trattare affari in concorrenza con l'imprenditore, sia per conto proprio che di terzi, mentre il secondo vieta al lavoratore di divulgare o di utilizzare, a vantaggio proprio o altrui, informazioni attinenti all'impresa, in modo da poterle arrecare danno[3].

Le "notizie" considerate nell'art. 2105 c.c. sotto il duplice profilo del divieto di uso e del divieto di divulgazione si identificano con le acquisizioni e informazioni - tecniche, applicative, di esperienza - estrinseche e oggettive rispetto al prestatore e alla sua personalità, che attengono al patrimonio immateriale dell'impresa, nella sua organizzazione e nei sistemi di produzione adottati.

Dal punto di vista penale vengono invece in rilievo gli artt. 615-ter, 622 e 623 c.p.

La prima disposizione, rubricata "Accesso abusivo ad un sistema informatico o telematico"[4] tutela il bene giuridico della riservatezza dei dati e dei programmi contenuti in un sistema informatico, messa in pericolo dalle intrusioni di soggetti non autorizzati.

Ai fini dell'art. 615-ter c.p. per "sistema informatico" si intende una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione

[1] Studio legale Comellini.

[2] *"Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio".*

[3] Tanto che *"è legittimo il licenziamento del lavoratore che comunichi a terzi le 'password' personali idonee a consentire l'accesso ad informazioni aziendali destinate a restare riservate"* (Cass. civ., 13.9.2006 n. 19554).

[4] Art. 615-ter c.p.: *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. […]".*

automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. Pertanto, non lo è tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire od elaborare dati in vista dello svolgimento di una funzione (si è escluso dunque il reato nel caso di riproduzione di dati di una banca dati contenuta in un sito non protetto da alcun sistema di sicurezza e in relazione al quale non risulta essersi verificata alcuna intrusione)[5].

D'altro canto, "sistema telematico" è, secondo una tesi estensiva, ogni forma di telecomunicazione che si giovi dell'apporto informatico per la sua gestione oppure che sia al servizio di tecnologie informatiche, indipendentemente dal fatto che la comunicazione avvenga via cavo, via etere o con altri sistemi. Per un orientamento minoritario si tratta, invece, essenzialmente delle forme di comunicazione tra computer via linea telefonica.

Per la sussistenza del reato è quindi necessario verificare, da un lato, se la condotta posta in essere dal dipendente o dal soggetto terzo rivesta i caratteri dell'abusività; dall'altro, se il sistema informatico o telematico sia protetto da misure di sicurezza tali da impedirne l'accesso.

La Suprema Corte ha, infatti, avuto modo di precisare come "*non commetta il reato di accesso abusivo ad un sistema informatico o telematico il soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga, sia pure per finalità illecite, fermo restando che egli dovrà comunque rispondere dei diversi reati che risultino eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate*"[6]. In altre parole, se il soggetto, lavoratore dipendente o meno, è autorizzato ad accedere al sistema ed a mantenersi all'interno dello stesso, senza alcuna limitazione temporale o di sicurezza, non viene superata alcuna protezione informatica.

I dati aziendali ricevono ulteriore tutela dalla diversa disposizione di cui all'art. 622 c.p., per cui chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo riveli, senza giusta causa, ovvero lo impieghi a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

Qui entra in gioco, una tutela più specifica, quella concernente quanto di segreto conosciuto e trasmesso nel rapporto anche tra cliente e professionista.

Nel binomio "professione o arte" si ricomprende ogni attività lavorativa o di prestazione di servizi svolta in favore di chi ne faccia richiesta o ne abbia necessità, svolta anche in via non esclusiva ma con carattere di continuità, per lo più remunerata. L'affiancamento dei due termini porta a ricomprendere qualsiasi attività di carattere intellettuale o manuale, dalle professioni liberali alle prestazioni d'opera del lavoratore subordinato. Non è necessario che le professioni abbiano un riconoscimento legale e siano disciplinate normativamente. Sono ricompresi in questa categoria, a titolo esemplificativo, gli avvocati, i commercialisti, i medici, le levatrici, i farmacisti, i giornalisti, gli istitutori, i domestici, e ovviamente anche i periti industriali.

Il segreto qui in esame, pur di difficile definizione, deve essere comunque interpretato in senso oggettivo e sostanziale, ricondotto a quelle ipotesi in cui la rivelazione delle notizie segrete potrebbe arrecare un danno ("nocumento") attuale o potenziale, dipendente dalla natura della notizia e, dunque, dalla sua relazione con la sfera intima del soggetto costretto a ricorrere al professionista.

Rispetto al disposto dell'art. 622 c.p. la fattispecie di reato prevista al successivo art. 623 ha carattere di specialità. Il segreto conosciuto e rivelato – da diversi soggetti ivi compresi, anche in questo caso, i professionisti - deve avere natura commerciale o essere relativo a scoperte o invenzioni scientifiche.

In questo caso, è necessario stabilire se quanto

[5] Trib. Milano 19.3.2007.

[6] Cass. pen., 29.5.2008 n. 26797.

sottratto dal dipendente (costituente il *know-how* aziendale) debba ricondursi o meno a "*notizie destinate a rimanere segrete*", così come previsto dalla fattispecie.

La Cassazione[7] nel pronunciarsi sul reato di cui all'art. 623 c.p., ha specificato i confini del bene giuridico tutelato dalla norma incriminatrice, affermando innanzitutto che non costituisce condizione necessaria la sussistenza dei presupposti di brevettabilità della scoperta o dell'applicazione rivelata, dovendosi ritenere "*oggetto della tutela penale del reato in questione il 'segreto industriale' in senso lato, ovvero quell'insieme di conoscenze riservate e di particolari modus operandi in grado di garantire la riduzione al minimo degli errori di progettazione e realizzazione e dunque la compressione dei tempi di produzione*".

In tema di rivelazione ed impiego di notizie destinate a rimanere segrete ai sensi dell'art. 623 c.p., non è richiesto ai fini della configurabilità del reato che le notizie de *quibus* siano originali o nuove in quanto le stesse ben possono essere costituite anche dal c.d. *know-how* aziendale inteso come il complesso di informazioni industriali necessarie per la costruzione, l'esercizio e la manutenzione di un impianto[8].

La copertura offerta dall'art. 623 c.p., quindi, è più ampia rispetto a quella predisposta dall'ordinamento civilistico all'invenzione brevettabile, estendendosi al patrimonio di conoscenze tecniche e organizzative acquisite negli anni dall'impresa, appunto il cd. *know how*.

Pertanto, sotto il profilo della responsabilità penale, la responsabilità si fonda sulla rilevanza e sullo spessore dei contributi tecnologici tutelati con il segreto, riguardo a cui rilevano in egual modo le condotte del dipendente e quelle di chi abbia conosciuto le notizie in forza di un rapporto non subordinato, ad esempio, il consulente esterno o il responsabile di altra impresa con cui sussista un rapporto di collaborazione che implichi l'acquisizione di notizie segrete. In particolare, vanno sottolineate le nuove esigenze del sistema produttivo, caratterizzato dallo sviluppo tecnologico e dalla divisione del lavoro, nonché le stesse esigenze della sicurezza del lavoro, che rendono necessari rapporti con una ampia cerchia di soggetti esterni all'impresa (consulenti, programmatori, tecnici della manutenzione ed assistenza, esperti della sicurezza), relazioni che hanno una funzione di particolare rilievo nei settori tecnologicamente più avanzati e che possono riguardare direttamente il perito industriale.

2. Obbligo del segreto professionale per il perito industriale.

Dall'esigenza di tutela del segreto, nelle varie accezioni che sopra si sono sinteticamente evidenziate, può derivare una responsabilità, non solo civile e penale, bensì anche deontologica, posto che per il professionista l'obbligo di segreto costituisce uno dei principi fondamentali la cui osservanza è necessaria ad assicurare la correttezza del rapporto fiduciario con il cliente. Per il perito industriale, l'obbligo trova una specifica previsione nell'art. 32 del vigente Codice deontologico.

La disposizione impone al perito industriale e perito industriale laureato il segreto professionale, anche nelle società tra professionisti di cui sia socio. Egli non può divulgare informazioni di cui sia venuto a conoscenza durante l'espletamento dell'incarico conferitogli, salvo il caso in cui sia espressamente autorizzato dal committente o per quanto è stabilito dal già citato art. 622 c.p.

L'obbligo sussiste durante il mandato e permane anche dopo la cessazione del rapporto con il committente.

Il professionista deve anche vigilare che i collaboratori, i dipendenti e i tirocinanti mantengano anch'essi il segreto professionale. In detto ultimo caso, se l'obbligo viene violato, egli risponderà anche del fatto di terzi, ai sensi degli artt. 1228 e 2049 c.c.

In ogni caso, dalla violazione del dovere di segreto può derivare l'applicazione di sanzioni disciplinari proporzionate alla gravità della condotta e all'entità delle informazioni diffuse.■

[7] Cass. pen., 4.6.2020 n. 16975.
[8] Cass. pen., 20.6.2001 n. 25008.