Direttiva (UE) 2016/943 sulla protezione del Know-How e delle informazioni commerciali riservate

La **Direttiva (UE) 2016/943** del Parlamento Europeo e del Consiglio, adottata l'8 giugno 2016, rappresenta un passo fondamentale nella protezione del **know-how** e delle **informazioni commerciali** riservate all'interno dell'Unione Europea. Questa direttiva mira a uniformare le legislazioni degli Stati membri riguardo alla tutela dei segreti commerciali, garantendo un quadro giuridico coerente ed efficace.

Il provvedimento introduce novità importanti e al contempo rafforza le misure già esistenti per la difesa del know-how aziendale e dei segreti commerciali.

In Italia invece la direttiva è stata recepita con il Decreto legislativo, **11/05/2018 n° 63** e si inserisce, in particolare, nella tutela già accordata alle informazioni segrete dagli articoli **98** e **99 Codice della Proprietà Industriale** (CPI).

Definizione di segreto commerciale e misure per la sua protezione

Il know-how aziendale e i segreti commerciali sono intesi sempre come "le informazioni aziendali, le esperienze tecnico-industriali, comprese quelle commerciali".

Al fine di poter beneficiare della tutela prevista dalla direttiva Europea e dal Codice della proprietà industriale, il know-how aziendale e i segreti commerciali devono soddisfare i

seguenti criteri:

- **Segretezza**: l’informazione non è generalmente nota o facilmente accessibile agli esperti e agli operatori del settore.
- **Valore economico**: l’informazione possiede un valore commerciale proprio in virtù della sua segretezza.
- **Misure di protezione**: il detentore dell’informazione ha adottato misure ragionevoli per mantenerla segreta.

Questi criteri sono essenziali per qualificare un’informazione come segreto commerciale e, di conseguenza, per garantirne la protezione legale.

La direttiva stabilisce che il concetto di «segreto commerciale» debba includere sia le informazioni di natura commerciale che quelle tecnologiche, a condizione che vi sia un legittimo interesse alla loro riservatezza. Inoltre, tali conoscenze o dati devono possedere un valore economico, attuale o potenziale.

Questo valore si manifesta, ad esempio, quando l’acquisizione, l’uso o la divulgazione non autorizzati potrebbero arrecare un danno alla persona fisica o giuridica che ne detiene legittimamente il controllo, compromettendone il potenziale scientifico e tecnologico, gli interessi finanziari e commerciali, le strategie aziendali o la competitività. Tuttavia, la definizione di segreto commerciale non comprende informazioni di scarso rilievo, l’esperienza e le competenze acquisite dai lavoratori nell’ambito della loro normale attività lavorativa, né le informazioni già note o facilmente accessibili agli operatori del settore di riferimento.

La direttiva stabilisce le regole per l’acquisizione, l’utilizzo e la divulgazione dei segreti commerciali, definendo in particolare le modalità attraverso cui è possibile ottenere tali informazioni in modo lecito. Tra i metodi consentiti rientrano la scoperta indipendente dello

stesso know-how e l'ingegneria inversa (**reverse engineering**). In particolare, l'acquisizione di un segreto commerciale è considerata legittima quando avviene mediante l'osservazione, l'analisi, lo smontaggio o la sperimentazione di un prodotto o di un oggetto che sia stato reso accessibile al pubblico o che sia legalmente in possesso di chi acquisisce le informazioni.

La Direttiva 2016/943, negli articoli **4** e **5**, stabilisce quali siano le modalità illecite di acquisizione, utilizzo e divulgazione di un segreto commerciale senza il consenso del legittimo detentore. Inoltre, l'uso o la diffusione non autorizzati di tali informazioni sono considerati illeciti se derivano da un'acquisizione ottenuta in modo illegittimo.

Tuttavia, la direttiva prevede alcune eccezioni che rendono lecita la divulgazione di un segreto commerciale. Tra queste rientra il cosiddetto **whistleblowing**, ovvero il caso in cui la rivelazione o l'utilizzo del segreto siano finalizzati a denunciare una condotta scorretta, un'irregolarità o un'attività illecita. Affinché questa eccezione sia applicabile, è necessario che l'autore della divulgazione abbia agito con l'intento di tutelare l'interesse pubblico generale (art. 5, par. 1, lett. b).

Per proteggere efficacemente i segreti commerciali, le aziende sono allora incoraggiate a adottare una serie di misure preventive, tra cui:

- **Implementazione di politiche interne di riservatezza**: stabilire linee guida chiare su come gestire e proteggere le informazioni sensibili.
- **Formazione del personale**: educare i dipendenti sull'importanza della protezione dei segreti commerciali e sulle procedure da seguire.
- **Utilizzo di accordi di non divulgazione (NDA)**: stipulare contratti che obbligano legalmente le parti a non divulgare informazioni riservate.
- **Controllo degli accessi**: limitare l'accesso ai dati

sensibili solo al personale autorizzato.

L’adozione di queste misure non solo aiuta a proteggere le informazioni riservate, ma rafforza anche la posizione legale dell’azienda in caso di controversie relative alla divulgazione non autorizzata di segreti commerciali.

Azioni legali per la violazione dei segreti commerciali

La Direttiva (UE) 2016/943 prevede strumenti legali specifici per affrontare la violazione dei segreti commerciali. In caso di appropriazione indebita o divulgazione non autorizzata, il detentore del segreto commerciale ha il diritto di intraprendere le opportune azioni legali per proteggere i propri interessi.

La direttiva prevede che le misure di protezione adottate siano **giuste**, **efficaci** e capaci di scoraggiare le violazioni, evitando al contempo costi eccessivi o procedure troppo complesse. Inoltre, nell’applicazione di tali tutele, è necessario garantire un equilibrio tra gli interessi coinvolti, assicurando che non vengano utilizzate in modo abusivo.

Le possibili azioni legali includono:

- **Misure cautelari**: richiesta di provvedimenti urgenti per prevenire l’ulteriore divulgazione o utilizzo del segreto commerciale, come ordini di cessazione o sequestro di materiali contenenti le informazioni riservate, le quali possono però essere revocate qualora l’attore non avvii un procedimento sul merito della violazione entro un termine ragionevole. Nei procedimenti cautelari, il giudice può consentire al presunto responsabile della violazione di continuare a utilizzare il know-how aziendale o i segreti commerciali

contestati, a condizione che venga versata una cauzione. Se la violazione è avvenuta senza dolo o colpa, l'autore può richiedere di proseguire l'uso delle informazioni riservate, offrendo appunto una cauzione proporzionata al valore delle royalty che sarebbero state dovute per un utilizzo legittimo del segreto commerciale. Tuttavia, la decisione finale spetta al giudice, che deve valutare attentamente tutte le circostanze del caso.

- **Risarcimento dei danni**: richiesta di compensazione finanziaria per i danni subiti a causa della violazione, che può includere la perdita di profitti, il danno all'immagine aziendale e altri costi correlati.
- **Distruzione o restituzione dei materiali**: richiesta di eliminazione, distruzione o restituzione di documenti, file o altri supporti contenenti il segreto commerciale.

Il **termine di prescrizione** delle violazioni dei diritti e delle azioni per chiedere l'applicazione delle misure di tutela viene fissato dalla direttiva in **6 anni** (art. 8).

È importante notare che, per avere successo in un'azione legale, il detentore del segreto commerciale deve dimostrare che l'informazione in questione soddisfa i criteri di segretezza, valore economico e che sono state adottate misure ragionevoli per mantenerla confidenziale.

Inoltre, la direttiva prevede che le azioni legali siano proporzionate e non ostacolino la concorrenza leale. Ciò significa che le misure adottate devono essere equilibrate e non devono limitare indebitamente le attività commerciali legittime.

Sono previste anche maggiori garanzie nei procedimenti giudiziari, infatti le aziende godono di maggiori tutele quando il procedimento riguarda segreti commerciali o know-how. Per garantire la riservatezza, il giudice può imporre ai soggetti coinvolti nel processo (come le parti, i legali e i consulenti tecnici) il divieto di divulgare o utilizzare le

informazioni riservate apprese durante il procedimento.

Inoltre, può ordinare l'oscuramento o la rimozione di dati sensibili dai documenti ufficiali. In caso di violazione di tali disposizioni, sono previste specifiche sanzioni penali. In particolare, il Decreto Legislativo n. 63/2018 attuativo della Direttiva Europea in esame, ha introdotto un inasprimento delle sanzioni per la divulgazione illecita di segreti commerciali o know-how aziendale ottenuti in modo improprio. Più precisamente, prevede pene severe, tra cui la reclusione fino a due anni. Inoltre, se l'infrazione viene commessa utilizzando strumenti informatici, la pena può essere ulteriormente aggravata.

Diritto all'informazione e alla libertà di espressione

La protezione dei segreti commerciali deve essere bilanciata con altri diritti fondamentali, come il diritto all'informazione e la libertà di espressione. La Direttiva (UE) 2016/943 riconosce l'importanza di questo equilibrio e prevede specifiche eccezioni alla protezione dei segreti commerciali.

Le principali eccezioni includono:

- **Libertà di espressione e di informazione**: la direttiva garantisce che la protezione dei segreti commerciali non possa essere invocata per limitare l'attività giornalistica o per impedire ai media di investigare e riportare notizie di interesse pubblico. Se la divulgazione di un segreto commerciale avviene nell'ambito di un'inchiesta giornalistica e risponde a un interesse collettivo rilevante, essa può essere considerata legittima, purché sia giustificata e proporzionata. Ciò significa che, nei casi in cui la rivelazione di determinate informazioni sia essenziale

per informare il pubblico su questioni di rilevanza sociale, economica o politica, il diritto alla riservatezza aziendale può essere limitato.
- **Tutela dei lavoratori**: Un’altra eccezione importante riguarda la tutela dei lavoratori. La direttiva prevede che le norme sui segreti commerciali non possano impedire ai dipendenti di utilizzare le informazioni acquisite nel corso del proprio impiego per esercitare i loro diritti. Questo è particolarmente rilevante nei casi di controversie lavorative, in cui i lavoratori potrebbero dover fare riferimento a conoscenze riservate per dimostrare il proprio caso, ad esempio in situazioni di licenziamenti ingiusti, discriminazioni o altre violazioni contrattuali. Tuttavia, questa eccezione non consente una divulgazione indiscriminata delle informazioni, ma solo nella misura strettamente necessaria alla tutela dei diritti del lavoratore.

Queste eccezioni garantiscono che la protezione dei segreti commerciali non venga utilizzata in modo abusivo per sopprimere la libertà di espressione, impedire la divulgazione di illeciti o limitare i diritti dei lavoratori.

Come le aziende possono tutelare il proprio know-how

La protezione efficace del know-how e delle informazioni commerciali riservate richiede un approccio strategico che coinvolga sia misure legali che operative. Le aziende devono adottare una politica di protezione del know-how che includa:

- **Analisi dei rischi**: identificare i dati sensibili e valutarne il livello di rischio. Questo processo prevede la mappatura dei dati riservati, distinguendo tra segreti commerciali, dati strategici e informazioni tecniche, oltre alla valutazione del livello di rischio legato a ciascuna tipologia di dato. L’azienda deve

considerare il valore economico dei dati, la loro esposizione a minacce interne o esterne e la possibilità di furto o divulgazione illecita.

- **Piani di sicurezza**: implementare misure di sicurezza fisiche e digitali per proteggere i dati aziendali. La protezione fisica delle informazioni prevede il controllo dell'accesso ai documenti e ai dispositivi sensibili attraverso sistemi di badge elettronici, telecamere di sorveglianza e locali riservati. Dal punto di vista informatico, è fondamentale implementare tecnologie avanzate come crittografia, firewall, VPN e autenticazione a più fattori per proteggere i dati digitali da attacchi esterni. È inoltre importante limitare l'accesso alle informazioni riservate solo ai dipendenti che ne hanno effettivamente bisogno, assegnando autorizzazioni in base ai ruoli.
- **Monitoraggio continuo**: verificare periodicamente l'efficacia delle misure adottate e aggiornare le strategie di protezione. La protezione del know-how deve essere un processo continuo e dinamico. È necessario monitorare e aggiornare costantemente le strategie di sicurezza, adeguandole alle evoluzioni normative e alle nuove tecnologie disponibili. Le aziende devono effettuare audit regolari per verificare l'efficacia delle misure adottate e utilizzare strumenti di monitoraggio avanzati per rilevare eventuali accessi non autorizzati o tentativi di sottrazione di dati riservati.

Un altro aspetto fondamentale è la formazione del personale, poiché i dipendenti rappresentano spesso l'anello più vulnerabile nella catena della sicurezza. È importante sensibilizzare tutti i collaboratori sull'importanza della protezione delle informazioni attraverso corsi di formazione periodici, in cui vengano illustrate le migliori pratiche di gestione dei dati aziendali e le procedure da seguire per prevenire il rischio di fughe di notizie. È inoltre essenziale

definire politiche aziendali chiare che regolino l’uso sicuro delle tecnologie, la gestione della documentazione riservata e le eventuali conseguenze in caso di violazione delle norme di riservatezza.

Seguendo queste pratiche, le aziende possono ridurre sensibilmente il rischio di furti di segreti commerciali e garantire la continuità del proprio vantaggio competitivo.

Conclusioni

La Direttiva (UE) 2016/943 rappresenta un’importante tappa nella tutela dei segreti commerciali e del know-how aziendale, armonizzando le normative degli Stati membri e fornendo strumenti concreti per la protezione delle informazioni riservate. L’adozione di misure preventive e una consapevolezza diffusa all’interno delle aziende sono essenziali per mitigare i rischi legati alla divulgazione non autorizzata. Tuttavia, il bilanciamento tra la protezione dei segreti commerciali e i diritti fondamentali, come la libertà di informazione e il whistleblowing, rimane cruciale per garantire un ambiente imprenditoriale equo e trasparente.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/direttiva-ue-2016-943/