DR. ERIC FALZONE – PADOVA 21 FEBBRAIO 2007

INFORMAZIONE & FORMAZIONE PRIVACY:

la conoscenza come principale misura minima di sicurezza

INDICE

INTRODUZIONE

I – LA DEFINIZIONE DI FORMAZIONE PRIVACY

II – LA REGOLA 19.6 DELL'ALLEGATO B)

III – SCOPI, FINALITA' E CARATTERISTICHE DELLA FORMAZIONE PRIVACY

IV – L'ANALISI E LA DETERMINAZIONE DEI BISOGNI FORMATIVI

V – LA PROGRAMMAZIONE DELLA FORMAZIONE PRIVACY

VI – LE FORME DI EROGAZIONE DELLA FORMAZIONE PRIVACY

VII – IL CONTROLLO E LA VALUTAZIONE DEI RISULTATI

VIII – LE RESPONSABILITA' CIVILI E PENALI PER MANCATA FORMAZIONE PRIVACY

CONCLUSIONI

FONTI

Privacy in Azienda: Manuale di Formazione per Titolari, Responsabili e Incaricati (Autore Eric Falzone – Casa Editrice Hoepli Spa) - Decreto legislativo 30 giugno 2003, n. 196 – D.P.R. 318/99 – Legge 675/96 – Quaderni CNIPA - Codice Civile –Codice Penale

Via A. Gloria 21 – 35030 Rubano (PD) – Tel. 348-6916273 – Fax 049-631246 – E-mail: eric.falzone@eucs.it

INTRODUZIONE:

"**Formare ed Informare**" un motto che dovrebbe connotare lo stile manageriale di ogni buon titolare, un approccio organizzativo che dovrebbe sempre guidare il vertice direzionale nelle difficili sfide dell'economia della conoscenza.

Purtroppo invece parlando di formazione privacy in azienda, il più delle volte ci si trova di fronte ad una lunga serie di preconcetti, che hanno la loro origine storica in un errato modello di sviluppo organizzativo aziendale e che trovano la loro logica in un consolidato sistema informativo e manageriale di tipo "*low cost*".

In questo contesto la formazione privacy viene spesso considerata dal top management come un oneroso costo ed un inutile bagaglio di conoscenze normative, che finisce per distogliere il personale dall'attività produttiva e per rallentare i processi aziendali con il rischio persino di creare possibili tensioni sindacali.

In realtà affrontando la problematica della formazione privacy in azienda con un corretto approccio psicologico, organizzativo e metodologico, si possono riscontrare fin da subito considerevoli vantaggi in termini di sicurezza e affidabilità dei sistemi informativi, di snellimento dei processi e delle procedure per la gestione documentale, di prevenzione di possibili reati informatici e trattamenti illeciti di dati personali con conseguente minore probabilità di richieste di risarcimento danni a titolo contrattuale o extracontrattuale.

La vera sfida per le aziende del nuovo millennio sarà quindi quella di riuscire a rinnovare costantemente i propri modelli organizzativi e cognitivi in maniera tale da imparare a formare ed informare il proprio personale su come affrontare i continui cambiamenti normativi, sociali e tecnologici nel rispetto di principi etici aziendali condivisi e basati sui diritti fondamentali dell'uomo, quali la privacy.

I - LA DEFINZIONE DI FORMAZIONE PRIVACY:

La "Formazione Privacy" può essere definita come "*l'insieme delle attività e degli interventi in materia di trattamento di dati personali e sicurezza delle informazioni, predisposti da un determinato titolare, finalizzati ad aumentare le competenze cognitive, operative e comportamentali di responsabili e incaricati ed in grado di incidere in maniera significativa sull'etica e le metodologie di lavoro aziendali."*

In particolar modo possono essere ricompresi nel concetto di "Formazione Privacy" tutti quegli interventi in materia di protezione di dati personali diretti a modificare abitudini comportamentali scorrette, a riconoscere pericoli e condizioni potenziali, che potrebbero determinare eventi indesiderati, a prevenire i rischi e a fronteggiare eventuali emergenze.

L'obbligo di formazione privacy, già presente in maniera implicita tra gli adempimenti previsti dalla legge 675/96, ha trovato un riconoscimento ufficiale solo con l'entrata in vigore del D.P.R. 318/99, con il quale veniva introdotto per la prima volta il "Documento Programmatico sulla Sicurezza" e, all'art. 6.1.d, "l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni."

II - LA REGOLA 19.6 – ALLEGATO B):

L'obbligo di formazione privacy, inizialmente introdotto con il DPR 318/99, verrà poi ripreso ed ampliato nel "Codice in Materia di Protezione dei Dati Personali" con l'introduzione della Regola 19.6 dell'Allegato B), che nel formulare i contenuti del Documento Programmatico sulla Sicurezza (DPS) prevede:

- *"interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;"*

Oltre che dalla Regola 19.6 dell'Allegato B), la formazione privacy come obbligo è ravvisabile anche in tutti quegli articoli del D.Lgs 196/03, nei quali il legislatore fa esplicito riferimento ai doveri del titolare di impartire istruzioni ai responsabili e agli incaricati del trattamento.

Il Codice Privacy individua, quindi, nella formazione lo strumento principe, che ogni titolare deve obbligatoriamente adottare, per aumentare la collaborazione di responsabili e incaricati e per ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nello specifico gli interventi formativi dovrebbero sempre focalizzarsi sulle scelte e sulle politiche aziendali in tema di privacy e sicurezza delle informazioni; con particolare attenzione alle esperienze quotidiane di lavoro in maniera tale da far emergere problematiche, rischi e comportamenti non corretti già presenti nelle operazioni di trattamento e individuare eventuali conoscenze mancanti, carenti o distorte.

Fondamentale per il buon esito degli interventi sarà poi un approccio formativo alla privacy ed alla sicurezza che superi la mentalità tradizionale legata al contingente e all'obbligo di un formale adeguamento ad un imperativo di legge. La formazione privacy dovrà essere quindi intesa ed affrontata come un processo di continuo e costante miglioramento, che non si limiti ad una semplice trasmissione teorica di informazioni, ma che coinvolga l'intera struttura organizzativa aziendale consentendo azioni programmatiche comuni e coordinate, che apportino a tutto il personale incaricato maggiori conoscenze ed abilità e soprattutto una maggiore consapevolezza dell'importanza dei propri comportamenti e del proprio ruolo funzionale.

III - SCOPI, FINALITA' E CARATTERISTICHE DELLA FORMAZIONE PRIVACY:

Come su evidenziato, la normativa ha imposto al titolare espliciti obblighi nel campo della formazione privacy. Questo ha generato nel tempo un'ampia e confusa offerta di servizi formazione, con il preoccupante risultato che molti titolari non riuscendo effettivamente a comparare e valutare la qualità delle offerte ed i risultati attesi, hanno basato la loro scelta unicamente sul parametro prezzo.

In questo modo l'obiettivo fondamentale del Codice Privacy, ovvero la promozione della cultura della sicurezza e della protezione dei dati personali, viene il più delle volte eluso a favore di un adempimento formale della norma, con il risultato che il personale incaricato al trattamento, invece di concentrarsi sull'apprendimento, tende di massima a mettere in pratica il minimo indispensabile per non incorrere nelle sanzioni previste per legge.

Per limitare questo fenomeno, è necessario quindi, che i titolari imparino a valutare e scegliere i servizi di formazione privacy in base a criteri e standard qualitativi largamente riconosciuti, tenendo almeno in considerazione che un progetto formativo corretto dovrebbe sempre prevedere:

- ✓ **un'analisi preliminare della domanda e dei bisogni formativi dei partecipanti;**
- ✓ **la definizione di obiettivi chiari, realistici e misurabili;**
- ✓ **l'adozione di metodi didattici efficaci e adeguati agli obiettivi, alle persone e alle risorse disponibili;**
- ✓ **l'utilizzo di docenti qualificati;**
- ✓ **una valutazione dei risultati raggiunti in termini di apprendimento.**

L'obiettivo della formazione privacy dovrebbe, quindi, essere quello di "creare un cambiamento effettivo" trasformando le attitudini di responsabili ed incaricati in capacità di agire, con interventi mirati ad aumentare le conoscenze specifiche e modificare atteggiamenti e comportamenti errati in modo da di diminuire (e nel lungo periodo annullare) il divario tra quanto pianificato in tema di misure di sicurezza nel DPS e quanto effettivamente attuato in azienda.

Un primo ostacolo da affrontare verso questo cammino risiede nella resistenza delle persone al cambiamento; il personale incaricato al trattamento è infatti reticente a modificare le proprie abitudini e modalità di lavoro o per pigrizia o perché si ritiene già perfettamente in grado di adempiere ai propri compiti senza la necessità di apprendere qualcosa di nuovo.

Prioritario è quindi agire in modo da far scomparire o attenuare queste resistenze individuando un metodo adeguato di informazione e formazione che non scaturisca solo dalle disposizioni di legge, ma sia parte integrante della filosofia e del codice etico aziendale .

L'errato od il mancato addestramento, infatti, si riflette sulle modalità di trattamento e più in generale sulla sicurezza dei dati personali, con aggravio del rischio di danni patrimoniali, derivanti da trattamenti illeciti dovuti a gestione di flussi informativi ridondanti ed inefficienti o a carenza di adeguate procedure organizzative ed operative.

Per queste ragioni gli interventi formativi, oltre a mirare ad ottemperare agli obblighi previsti dal D.Lgs 196/03, devono altresì essere flessibili ed adattarsi ai piani di addestramento eventualmente già esistenti in azienda.

Un adeguato percorso formativo privacy dovrebbe pertanto sempre prevedere le seguenti fasi di intervento:

- ✓ **Fase I - Informazione di base sui rischi generali esistenti in azienda**

  Tale informazione dovrebbe essere fornita a tutti i neoassunti in maniera da metterli in condizione di conoscere la struttura organizzativa in cui sono inseriti, gli aspetti più importanti del rapporto di lavoro e le principali procedure per il trattamento e misure minime di sicurezza adottate in azienda. In questa fase è indispensabile fornire gli elementi più importanti della normativa informando sui rischi generali dell'impresa e sensibilizzando e formando gli incaricati su come operare in termini di sicurezza e protezione dei dati personali.

- ✓ **Fase II - Formazione sui rischi specifici della mansione**

  Responsabili ed Incaricati dovrebbero poi ricevere formazione - sia in fase di assunzione che di successive variazioni del rapporto di lavoro - sui rischi specifici della mansione svolta, sulle misure di sicurezza adottate e da adottare, con esplicito riferimento a quanto previsto nel Documento Programmatico di Sicurezza per il ruolo da essi ricoperto. Questa fase della formazione dovrebbe essere realizzata mediante un approccio didattico che si avvalga di lezioni teoriche e tecniche di affiancamento in maniera tale da garantire ed assicurare l'effettiva trasmissione di conoscenze e procedure per il trattamento, nonché di tutte le misure di sicurezza definite dal titolare per una determinata mansione. La figura che si dovrà occupare dell'affiancamento dovrà essere una

persona già esperta in materia privacy, con competenze specifiche di ruolo e che sia al tempo stesso in grado di trasmettere oltre al know-how tecnico anche i valori etici aziendali.

- ✓ **Fase III - Formazione Continua e di Routine**

  Una formazione continua dovrebbe essere poi rivolta al personale incaricato, che ricopre la stessa posizione lavorativa da molto tempo e che per questo motivo può risentire di fattori quali l'assuefazione, l'abitudine e la carenza di interesse nell'aggiornamento delle procedure di trattamento e delle misure minime di sicurezza aziendali. I cambiamenti normativi, tecnologici, organizzativi, logistici e procedurali, infatti, richiedono sempre un intervento formativo al fine di adeguare e motivare le persone alle novità.

IV - L'ANALISI E LA DETERMINAZIONE DEI BISOGNI FORMATIVI PRIVACY:

La prima fase di un progetto formativo privacy dovrebbe essere rivolta all'analisi e alla determinazione dei bisogni formativi in ambito privacy ed in particolare alla fine di questa fase dovrebbero essere note al titolare le seguenti informazioni:

- ✓ **Figure chiave da coinvolgere**
- ✓ **Materie da trattare**
- ✓ **Metodologie didattiche da utilizzare**
- ✓ **Eventuali argomenti pertinenti di interesse da trattare**

Queste informazioni potranno essere raccolte principalmente attraverso:

- ✓ **Osservazioni informali;**
- ✓ **Colloqui con Responsabili e Incaricati;**
- ✓ **Valutazione del contesto organizzativo e del grado di adeguamento dell'azienda agli obblighi normativi.**

In questa fase, un ruolo fondamentale dovrà essere inoltre affidato ai Responsabili Interni, che in qualità di supervisori dotati di autorità e preposti alla sorveglianza di determinati ambiti di trattamento dovranno partecipare agli interventi formativi e controllare i risultati delle azioni intraprese verificandone così l'efficacia. Questo in quanto, essendo nella migliore posizione di vedere e sentire cosa non va, sono in grado di agire in maniera più tempestiva ed efficace rispetto ad uno specialista della formazione.

V - LA PROGRAMMAZIONE DELLA FORMAZIONE PRIVACY:

Una volta individuati i bisogni formativi si dovrà procedere con la definizione di un programma didattico strutturato sulle specifiche esigenze delle varie aree aziendali.

Si potrà quindi optare per l'utilizzo di risorse esterne allo scopo di incamerare in azienda nuove competenze o decidere di avvalersi di risorse interne, qualora vi siano figure in azienda con tempo a disposizione e che conoscano il personale, il sistema informativo, la struttura organizzativa e le più moderne tecniche di apprendimento.

Si dovrà poi procedere alla redazione di un calendario di eventi formativi da sottoporre al vaglio e all'approvazione dei Responsabili Interni e del personale dirigente delle varie aree aziendali.

Lo sviluppo del percorso formativo potrà poi variare in funzione degli obiettivi prefissati in sede di analisi, e potrà consistere in:

- ✓ **Formazione in Aula**
- ✓ **Formazione E-learning**
- ✓ **Formazione a Distanza**
- ✓ **Formazione per Affiancamento**

Il materiale didattico utilizzabile invece potrà consistere a scelta in:

- ✓ **Manuali di Formazione Privacy**
- ✓ **Software Didattici**
- ✓ **Dispense o Letture Orientate**
- ✓ **Materiale Audiovisivo**
- ✓ **Simulazioni sul luogo di lavoro.**

VI - LE FORME DI EROGAZIONE DELLA FORMAZIONE PRIVACY:

Al fine di erogare corsi di formazione privacy che risultino efficaci, ogni titolare dovrà tenere in considerazione tre parametri fondamentali:

- ✓ **La metodologia didattica da adottare**
- ✓ **I contenuti da trattare durante il corso**
- ✓ **La tipologia di esercitazioni da utilizzare in sede di valutazione**

Ognuno di questi parametri dovrà essere valutato tenendo conto del ruolo, delle mansioni e dell'ambito di trattamento di affidato a ciascun incaricato, nonché delle specifiche procedure di trattamento adottate da ogni singola area aziendale.

Agli eventi formativi dovranno obbligatoriamente partecipare tutti i responsabili interni e tutte le persone incaricate al trattamento di dati personali indipendentemente dalla tipologia di dato trattato (sono infatti soggetti a formazione anche gli incaricati che trattano semplicemente dati personali comuni).

Il titolare potrà discrezionalmente optare per una o più delle seguenti metodologie didattiche:

- ✓ **Formazione in Aula**

  E' la modalità classica di fare formazione privacy; Essa prevede la pianificazione di eventi formativi, all'interno o all'esterno dell'azienda, tenuti da docenti competenti in materia di privacy e sicurezza delle informazioni. La figura del docente potrà essere selezionata tra consulenti esterni o personale interno appositamente addetto alla formazione (è comunque preferibile almeno per la "Fase I - Informazione di base sui rischi generali esistenti in azienda" utilizzare docenti esterni che possano, in caso di eventuali successivi contenziosi con il lavoratore, certificare l'avvenuta formazione privacy). Il ruolo del docente dovrà principalmente essere quello di

coordinatore e mediatore tra esigenze formative imposte dalla legge (con particolare attenzione all'effettivo recepimento delle misure minime di sicurezza adottate dal titolare) e la necessità di stimoli motivazionali da parte di tutti i partecipanti.

✓ **E-learning**

Altra modalità di formazione privacy molto diffusa è quella definita di "e-learning" ovvero basata su sistemi che sfruttano le potenzialità di internet per fornire formazione distribuendo contenuti didattici multimediali on-line, in maniera tale che più utenti possano accedere ai contenuti dei corsi in ogni luogo ed in qualsiasi momento. L'e-learning non deve essere confuso con altre tipologie di formazione, anch'esse erogate tramite tecnologia informatica (quali ad esempio: Computer Based Training" - C.B.T.), che appartengono invece alle tecniche definite di formazione a distanza (FAD). La formazione privacy con modalità e-learning non deve comunque mai essere considerata un'alternativa alla formazione tradizionale in aula, ma deve piuttosto essere concepita come un'integrazione o un suo logico completamento. Un progetto formativo in modalità e-learning presenta implicazioni di ordine organizzativo, tecnologico e metodologico, che comportano importanti investimenti iniziali e deve, quindi, essere attentamente monitorato e valutato nei vari stadi di sviluppo. I fattori che occorre analizzare per progettare un intervento formativo privacy on-line sono principalmente: la dimensione dell'azienda, la sua estensione a livello territoriale, il suo settore di appartenenza, il suo stadio di informatizzazione e il livello di alfabetizzazione informatica dei destinatari. In un processo di e-learning infine la formazione deve essere intesa come un percorso interattivo in cui l'utente deve partecipare attivamente.

✓ **Formazione a Distanza**

Le tecniche di Formazione a Distanza (FAD) nascono per superare i problemi spazio-temporali tipici della formazione in aula, che richiedono la presenza contemporanea di più persone nello stesso luogo per un medesimo periodo di tempo. Rispetto alla modalità tradizionale in aula, la FAD presenta il notevole vantaggio di poter personalizzare la formazione a seconda dell'utente, del luogo e del tempo a disposizione. Anche qui come per l'e-learning il suo utilizzo deve essere considerato secondario e marginale rispetto alla formazione classica in aula, che dovrebbe sempre essere considerata la modalità di erogazione primaria della formazione privacy in azienda. Tra le principali forme di formazione a distanza troviamo i sistemi cosiddetti "Computer Based Training" - C.B.T" ovvero metodi di insegnamento basati sull'uso di speciali programmi didattici per computer o di altro software dedicato fornito su supporti CD-ROM o DVD-ROM. I metodi CBT hanno però l'enorme svantaggio di poter essere utilizzati esclusivamente con l'ausilio di strumenti elettronici. Per risolvere questo problema (ed in particolar modo nei casi in cui sia necessario formare incaricati al trattamento singolarmente e in maniera svincolata dall'utilizzo di sistemi informatici) si propone l'adozione di un nuovo metodo di formazione a distanza basato sul manuale e prontuario *"Privacy in Azienda: Manuale di Formazione per Titolari, Responsabile e Incaricati"* (Editore: Casa Editrice Libraria Ulrico Hoepli Spa - Autore: Eric Falzone - Pag. 133 – Prezzo di Copertina: € 13,00) un'opera strutturata per essere utilizzata sia come manuale di formazione privacy che come vademecum tascabile per l'adempimento degli obblighi normativi previsti dal Codice Privacy. La modalità formativa a distanza proposta nel manuale "Privacy in Azienda" prevede 4 fasi di intervento:

- Fase I: individuazione a cura del titolare/responsabile (con il supporto eventualmente anche di un consulente privacy esterno) delle necessità di formazione di ciascun incaricato;
- Fase II: consegna di una copia del manuale di formazione "Privacy in Azienda" a ciascun incaricato con l'indicazione delle sezioni da studiare;
- Fase III: erogazione di un test di verifica dell'apprendimento dell'incaricato (tramite gli appositi questionari presenti nel manuale "Privacy in Azienda") e successiva correzione e valutazione dei risultati da parte del titolare/responsabile (con eventuale supervisione di un consulente privacy esterno);
- Fase IV: utilizzo del manuale - da lasciare in dotazione ad ogni singolo incaricato - come vademecum tascabile da consultare in caso di dubbi o problemi.

I principali vantaggi riscontrati dai titolari che hanno utilizzato il metodo di formazione a distanza basato sul manuale "Privacy in Azienda" sono stati: il completo adempimento degli obblighi di formazione imposti dalla legge, l'abbattimento dei costi di formazione, l'ottenimento di un feedback immediato sull'apprendimento degli incaricati e la possibilità di mettere a disposizione del personale uno strumento operativo immediatamente consultabile in caso di necessità.

VII - IL CONTROLLO E LA VALUTAZIONE DEI RISULTATI:

La fase successiva all'erogazione della formazione privacy è la valutazione dei risultati ottenuti in considerazione anche del loro possibile impatto in termini di analisi del rischio.

Questa fase risulta forse la più problematica da gestire in quanto, al fine di una corretta valutazione, si dovrà:

- ✓ stabilire a priori la "condizione di partenza" di ogni partecipante;
- ✓ calcolare il reale vantaggio acquisito da ogni incaricato in termini di conoscenze, capacità e modifiche di atteggiamento e comportamenti;
- ✓ soppesare il risultato complessivo ottenuto sia in termini prestazioni personali che di impatto sul contesto organizzativo del trattamento ai fini dell'analisi dei rischi.

Qualora, al termine di questo processo, i risultati finali non fossero soddisfacenti, si dovrà procedere alla riformulazione e ripetizione degli eventi formativi e non si potrà inserire l'incaricato nell'organizzazione fintanto che non sia stato valutato idoneo.

Un corretto processo di valutazione dovrebbe quindi essere svolto prima, durante e dopo il processo formativo e dovrebbe comprendere una:

- ✓ **Valutazione Preliminare:** diretta ad individuare caratteristiche personali e punti di forza/debolezza
- ✓ **Valutazione Intermedia di Apprendimento:** volta a misurare il grado di apprendimento in fase di erogazione della formazione privacy
- ✓ **Valutazione Formativa Finale:** diretta a verificare il livello di apprendimento finale acquisito e la predisposizione degli incaricati all'applicazione delle novità oggetto della formazione
- ✓ **Valutazione Permanente**: volta ad una verifica periodica – con cadenza almeno annuale anche contestualmente all'aggiornamento del Documento Programmatica sulla Sicurezza - sull'adeguatezza della formazione privacy svolta e sul livello di applicazione di procedure e misure minime di sicurezza adottate dal titolare.

VIII - LE RESPONSABILITA' CIVILI E PENALI PER MANCATA FORMAZIONE PRIVACY:

Come finora evidenziato, la formazione privacy è un obbligo di legge sia in termini di generale misura di sicurezza (art. 31) che di particolare misura minima di sicurezza (art. 33, 34 e 35).

Le scelte attinenti alle modalità di erogazione della formazione privacy, invece, hanno natura discrezionale e sono liberamente valutabili dal titolare in base ai bisogni formativi degli incaricati, alle procedure aziendali e alle misure minime di sicurezza adottate per il trattamento.

Qualora il titolare non provveda a formare il personale incaricato, potrà perciò essere penalmente perseguito per il reato - previsto all'art. 169 del D.Lgs 196/03 - di omessa adozione di misure minime di sicurezza con conseguente possibile arresto sino a due anni o ammenda da € 10.000,00 a € 50.000,00.

Inoltre potrà vedersi costretto anche a rispondere per gli eventuali danni cagionati a terzi per effetto delle operazioni di trattamento per il semplice fatto di non aver adottato tutte le misure di sicurezza idonee a ridurre al minimo il rischio. Nello specifico il Codice Privacy all'art. 15.1 prevede che:

- ✓ *"Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile."*

Con il riferimento all'art. 2050 c.c. (che disciplina la figura del risarcimento del danno per fatto illecito - art. 2043 c.c. - in caso di responsabilità per esercizio di attività pericolose) il legislatore ha perciò esplicitamente dichiarato il trattamento dei dati personali un attività pericolosa.

Pertanto il titolare che cagioni danno ad altri per effetto del trattamento di dati personali sarà "…*tenuto al risarcimento se non prova di aver adottato tutte le misure idonee a evitare il danno*" tra le quali anche e soprattutto la formazione privacy. Sarà quindi a carico del titolare l'onere della prova ovvero dimostrare di avere adottato tutte le misure idonee ad evitare il danno, compresa anche la formazione privacy. Al titolare che voglia esimersi dal risarcimento, non sarà sufficiente affermare di non avere violato le disposizioni di legge (cosiddetta prova negativa), ma dovrà dimostrare necessariamente di avere adottato tutte le misure possibili per impedire l'evento dannoso (cosiddetta prova positiva). Tale dimostrazione risulterà fondata solo qualora dimostri che tra l'attività di trattamento e l'evento dannoso non ci sia un nesso di causalità.

Secondo l'orientamento prevalente della Cassazione, la responsabilità sarà imputata a chi, al momento del danno, esercitava il controllo sull'attività di trattamento. L'imprenditore pertanto è tenuto ad organizzare le attività di trattamento in maniera tale da poter ricondurre gli eventi dannosi ai soli episodi di caso fortuito. Al fine di ottenere il risarcimento, l'interessato dovrà solamente provare che il danno si sia effettivamente realizzato e che sia dipeso dall'attività di trattamento posta in essere sotto il controllo del titolare. Per sottrarsi dall'obbligo di risarcimento, il titolare avrà, invece, l'onere di provare di avere adottato tutte le misure idonee a evitare il danno, compresa la formazione privacy.

Qualora il danno sia dovuto a negligenza o errore imputabile ai responsabili o al personale incaricato, il titolare per rivalersi su di essi dovrà provare di aver adottato tutte le cautele del caso, ed in particolare di aver effettuato una corretta formazione privacy mirata alla conoscenza delle disposizioni di legge, all'utilizzo degli strumenti e delle risorse aziendali, e all'apprendimento delle procedure e delle misure minime di sicurezza previste per il trattamento dei dati personali. Inoltre dovrà provare di aver selezionato accuratamente le modalità formative più idonee, di aver erogato adeguatamente la formazione e di aver vigilato costantemente sull'operato di responsabili ed incaricati anche al termine degli eventi formativi.

Quindi il titolare che abbia effettuato una corretta formazione privacy - in caso di violazione da parte di responsabili e incaricati delle disposizioni impartite e degli obblighi di fedeltà (art. 2105 c.c.) e diligenza (art. 2104 c.c.) - oltre ad applicare le sanzioni disciplinari previste (art. 2106 c.c.) potrà rivalersi sui lavoratori inadempienti richiedendo il risarcimento dei danni subiti.

Il lavoratore che sia stato edotto "…*dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare*…" risponde perciò del danneggiamento a titolo di responsabilità contrattuale e, precisamente, a titolo di inadempimento dell'obbligo di diligenza nell'esecuzione della prestazione di lavoro. Ai fini della richiesta di risarcimento del danno fondata sulla responsabilità contrattuale per inadempimento, il titolare può inoltre anche non rispettare le procedure previste dall'art. 7 dello Statuto dei Lavoratori, in quanto esse mirano a limitare l'esercizio unilaterale del potere disciplinare da parte del datore di lavoro, e non a disciplinare l'ipotesi di azione di responsabilità per inadempimento ai sensi dell'art 1218 c.c.

Al fine del risarcimento del danno, tuttavia incombe sul titolare l'onere di fornire la prova (che deve essere autonomamente e concretamente dimostrata) che l'evento dannoso sia da riconnettere ad una condotta colposa del personale incaricato, derivante da una violazione degli obblighi di diligenza.

CONCLUSIONI:

Da quanto finora evidenziato, la formazione privacy, più che un obbligo normativo, dovrebbe essere considerata dai titolari un'irripetibile opportunità per trasmettere i valori etici aziendali e per coinvolgere il personale nelle scelte organizzative e gestionali, creando così una politica di sicurezza comunemente condivisa.

Affinchè ciò si avveri, è però indispensabile un radicale mutamento di mentalità da parte dei vertici aziendali ed un conseguente reindirizzamento degli stili manageriali verso schemi organizzativi aperti e partecipativi tipici dell'economia della conoscenza.

La formazione, pertanto, non dovrebbe essere più considerata un costo, ma un logico ed indispensabile strumento per modellare i processi organizzativi e garantire la condivisione di una filosofia etica aziendale basata sui valori della protezione dei dati personali e della sicurezza delle informazioni.