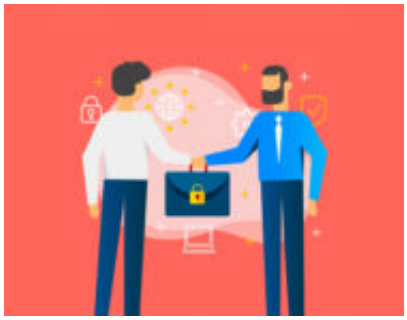
La consulenza privacy ed il rapporto con il cliente

Author : Giuseppe Diretto

Date : 11 Febbraio 2019



Fiducia… ma quanta fatica

Dopo qualche mese di attività di consulenza in ambito privacy ai tempi del GDPR, abbiamo pensato di fare un **primo bilancio**, con l'obiettivo di fornire anche **spunti di riflessione** a molti colleghi che faticano a trovare il *bandolo della matassa* nel rapporto con il cliente in questo particolare ambito.

Cominciamo a tracciare alcune **differenze** tra la consulenza in materia di privacy e gli ambiti consulenziali tradizionali:

- la protezione dei dati **non ha scadenze**: non prevede, cioè, la trasmissione della dichiarazione dei redditi telematica (consulente tributario), la produzione delle buste paga (consulente del lavoro) o il progetto del nuovo archivio da presentare al Comando Provinciale dei Vigili del Fuoco (ingegnere); la privacy non si identifica con un prodotto finale, è impalpabile e, in buona parte, difficile da rappresentare concretamente;
- la protezione dei dati personali, eccettuate alcune prassi di riferimento UNI e le linee guida WP29 ed EDPB, **non ha standard metodologici** assoluti di riferimento, né ci sono, per il momento, albi professionali. Queste caratteristiche inducono spesso le organizzazioni ad affidare il compito della *compliance* alla normativa sulla privacy alle figure più disparate: per esempio, al capo del personale (nelle organizzazioni che ne hanno uno) oppure a chi presidia la *compliance* al Dlgs. 231/2001;
- **i dati personali da proteggere sono ovunque** e, quindi, in nessun posto specifico; non sono appannaggio esclusivo di una funzione aziendale o di una persona o di un ruolo, perché la loro presenza permea l'organizzazione.

Queste considerazioni incidono notevolmente sull'approccio che il consulente privacy deve avere con il cliente. Ci siamo convinti, infatti, che molto spesso il rapporto, almeno all'inizio, è molto simile a quello con il nonno riottoso che tossisce tutta la notte, ma non vuole farsi curare. La dinamica, infatti, si sviluppa in **quattro passaggi** delicati (simili a quelli da praticare con il nonno):

- convincere;
- analizzare;
- consigliare;
- verificare.

Cercheremo di approfondire le difficoltà che bisogna affrontare in ognuna di queste quattro fasi, anche per capire quali possano essere i comportamenti da adottare per evitare contrapposizioni poco proficue.

Convincere

Innanzitutto, il nonno non vuole andare dal medico. **Dice che è inutile, minimizza i sintomi** e, poi, un suo amico ha tossito per due settimane di seguito e, alla fine, tutto è passato senza alcuna cura. Il cliente ha un comportamento molto simile: qualche conoscente gli ha detto che "questa storia della privacy" è una moda che, ogni tanto, ritorna ma che, in fondo, non ha nessun effetto pratico. E, poi, nella sua azienda non si trattano "dati sensibili" (la tendenza a minimizzare prima di aver approfondito l'argomento) e, sentendo alcuni colleghi, nessuno si è mosso.

Qualcuno (come farebbe il nonno) **arriva persino a tentare l'automedicazione** e, con un giro su Internet, scarica qualche fac?simile per l'informativa o per la designazione dei soggetti autorizzati al trattamento.

Qualcun altro, invece, decide che è meglio farsi consigliare. Molti *consiglieri* ammettono, però, che "stanno per affrontare la questione ma non l'hanno ancora fatto" o, qualche volta, si trasformano in consulenti privacy improvvisati e forniscono i format che, a loro volta, hanno trovato su Internet.

Certo, **esistono anche imprenditori o dirigenti pubblici più accorti**, sensibili al buon andamento della loro organizzazione. **Ma, spesso, il budget disponibile è ridotto** oppure si fanno eterodirigere da qualche fornitore (tipicamente i fornitori di servizi ICT). Per esempio, in un avviso pubblico per la manifestazione di interesse di una società medio?piccola a partecipazione pubblica abbiamo potuto leggere, come requisito di capacità economica e finanziaria, che "il concorrente deve aver realizzato un fatturato globale minimo annuo riferito a ciascuno degli ultimi 3 (tre) esercizi finanziari disponibili di Euro 350.000 (IVA esclusa). Il settore di attività è *Produzione di software, consulenza informatica e attività connesse – Gestione di strutture informatizzate*". È come se il nonno accettasse di essere curato solo in una clinica Mességué.

Per convincere i clienti che **la protezione dei dati è un primario interesse dell'organizzazione** e che conviene farsi guidare da **professionisti capaci**, non basta neanche l'illustrazione degli aspetti sanzionatori. Quindi, nella nostra esperienza, abbiamo fatto leva su **due aspetti**: la **reputazione** e la **consapevolezza**.

La reputazione è importante, tanto per un albergo quanto per un ente pubblico, come un Comune. Abbiamo fatto l'esempio del turista straniero che ha il potere di danneggiare, con

qualche tweet, il brand che un albergo o una città si sono faticosamente costruiti nel tempo per il solo fatto di non aver ricevuto un'informativa (per esempio, dall'albergo) o perché gli sono stati richiesti dati non necessari (per esempio, nel corso di un controllo della Polizia Locale).

La consapevolezza arriva con qualche domanda mirata: "Lo sai che il tuo servizio telefonico di customer care chiede il numero di componenti del nucleo familiare? Perché lo chiede?" Oppure: "Lo sai che l'avviso che i vigili urbani del tuo comune lasciano sotto il tergicristallo corrisponde ad un trattamento che non ha basi giuridiche? E che qualche malintenzionato può approfittarne?"

In questo modo, molti "potenziali clienti" hanno messo a fuoco la questione, anche se **il percorso per arrivare in fondo**, dopo questa fase, **è ancora lungo**.

Analizzare

Una volta seduti al tavolo delle riunioni con i clienti, la seconda fase prevede che si debba aiutarli ad individuare ed analizzare i **processi di trattamento**. Il nostro approccio è semplice: di solito **partiamo da un documento aziendale che tutti conoscono** (o dovrebbero conoscere): la documentazione di riferimento del sistema di gestione della qualità, il "modello 231", il "Piano triennale per la prevenzione della corruzione e della trasparenza", ecc. (è meglio non prendere in considerazione il vecchio Documento Programmatico sulla Sicurezza perché troppo datato e, tradizionalmente, sempre mal digerito o addirittura sconosciuto). Partire da uno o più di questi documenti serve a *rompere il ghiaccio* con lo stato maggiore dell'organizzazione (dirigenti o funzionari responsabili di uffici) sia essa pubblica o privata. Serve a far capire loro che, nonostante l'analisi necessaria alla protezione dei dati personali sia una cosa diversa, abbiamo elementi di partenza che, in passato, loro stessi sono stati capaci di approfondire. Certo, qualcuno rimane stupito quando chiediamo di avere le copie delle planimetrie dei locali dove opera l'organizzazione: ma l'analisi deve essere condotta fino in fondo e, finalmente, si convincono che **la tenuta della *catena di protezione* dei dati personali si può valutare solo misurando la tenuta dell'anello più debole**, che può essere anche una stanza poco protetta.

Abbiamo trovato utile muoverci tra identificazione ed analisi dei processi di trattamento dei dati personali con l'impiego di **linguaggi visuali standard** (tipicamente il Business Process Model and Notation). Si costruisce, insieme allo stato maggiore aziendale, un **diagramma di flusso interfunzionale** per ogni ipotetico processo arricchendolo, tra le altre, con le seguenti **informazioni**:

- soggetti interni coinvolti nel trattamento;
- soggetti esterni coinvolti nel trattamento (quelli che diventeranno i responsabili *ex* art. 28 del GDPR e per i quali bisognerà rivedere attentamente le dinamiche contrattuali);
- basi giuridiche;
- dati trattati;
- strumenti utilizzati (sistemi di archiviazione cartacea, sistemi informativi interni, sistemi informativi esterni).

Modellare un diagramma visuale, tra le altre cose, aiuta a capire se il processo di trattamento è uno o più di uno: spesso nella testa di chi opera quotidianamente, si danno per scontate circostanze che, invece, scontate non sono. Per esempio, ci è capitato di analizzare un processo di raccolta di rifiuti “da incontinenza” su richiesta del cittadino. Dal punto di vista pratico la dinamica operativa è identica: il cittadino segnala che ci sono rifiuti da raccogliere e l’operatore ecologico, periodicamente, li preleva. Dal punto di vista dei dati personali, invece, i processi di trattamento sono due, con basi giuridiche completamente differenti visto che per i *pannolini* si trattava di acquisire e gestire dati personali *comuni* riferiti ai neonati mentre per i *pannoloni* gli interessati, aventi diritto al servizio, erano persone con patologie di incontinenza certificate da un medico. Con questa tecnica si arriva a completare, tenendole su binari paralleli, le fasi di identificazione e di analisi dei processi.

In molti casi, l’analisi effettuata concentrandosi sui dati personali **ha indotto il cliente** (titolare o responsabile del trattamento) **ad estendere la rivisitazione dei processi anche oltre le previsioni del GDPR**:

- con un ridisegno e, quindi, solo con qualche aggiustamento;
- con una reingegnerizzazione e, quindi, con un totale ripensamento di attività e flussi.

Dopo aver consolidato il diagramma, lo studio prosegue con l’**analisi del rischio**. Anche in questo caso non è semplice interagire con i **clienti** che, **di solito, tendono a minimizzare i rischi**; è un atteggiamento normale, dovuto all’istinto di difendere ciò che hanno costruito, spesso faticosamente, in termini di strumentazione, di prassi organizzative, di cultura aziendale. E, quindi, viene alla luce che:

- lo *switch* nel corridoio di un ospedale è il frutto dello sforzo di razionalizzazione fatto per aumentare il numero di posti letto;
- il dipendente che si occupa dei fascicoli del personale è eccellente, ma è troppo impegnato per tenere separati i documenti contenenti dati *comuni* dai documenti contenenti le particolari categorie di dati personali;
- la profilazione del sistema informativo prevede solo due livelli (lettura e lettura/modifica sull’intero patrimonio di dati) ma cambiare software significherebbe disorientare i dipendenti.

Inoltre, quando l’analisi va più in profondità, anche utilizzando specifici strumenti per *sondare* le misure di sicurezza informatiche, **si mette in discussione il lavoro**, spesso ingrato e faticoso, **di chi si occupa di conduzione e sviluppo ICT** all’interno dell’organizzazione: si tratta, di solito, di persone che hanno subìto tagli al budget ma che, in qualche maniera, sono riusciti a far funzionare la *ditta*.

Consigliare

Dall’analisi all’elaborazione del piano d’azione, con la dovuta indicazione degli interventi prioritari, il passo è breve. **È buona norma redigere il piano d’azione in stretta collaborazione con i dirigenti** dell’organizzazione. Questo ha alcuni vantaggi: si possono modulare meglio gli interventi sia in termini di efficacia sia con riferimento alla *reale* tempistica

necessaria. Ci sono, però, **alcuni svantaggi** (apparentemente di segno diverso):

- l'atteggiamento conservatore che il *management*, per varie ragioni, può assumere;
- l'occasione, *insperata*, da parte di qualche dirigente, di aumentare il budget disponibile per il semestre successivo.

Un approccio alternativo può essere quello di elaborare un piano d'azione senza il contributo del *management* e, successivamente, contrattarne il contenuto con la dirigenza senza, tuttavia, cedere troppo sull'efficacia finale degli interventi e, piuttosto, pianificando approcci graduali che possono costituire un compromesso tra l'*as is* ed il *to be*.

Nei nostri piani d'azione non mancano mai i **riferimenti alla formazione dei soggetti autorizzati** che, in qualche caso, è un insieme più ampio dei dipendenti (vedi, per esempio, i consiglieri comunali nel caso dei Comuni). D'altra parte **le statistiche ci dicono che circa il 70% delle violazioni derivano**, direttamente o indirettamente, **da comportamenti non corretti** da parte di chi opera all'interno delle organizzazioni (rispetto ad email di *phishing*, attacchi di ingegneria sociale, password ripetute, mancato rispetto del *clean desk*, ecc.)

Verificare

Anche la fase di verifica del rispetto del GDPR e delle policy interne *autodefinite* crea qualche problema al cliente. **Le organizzazioni già certificate rispetto a standard ISO sono abituate** a questo approccio e, quindi, risentono poco dei riscontri che occorre fornire periodicamente; **le altre**, soprattutto quelle medio?piccole, **vivono l'azione di verifica come un intralcio alle "dinamiche di business quotidiane"** piuttosto che come un doveroso *pit?stop* per capire se ci sono elementi non sufficientemente integrati o ulteriori margini di miglioramento.

Non dimentichiamo, inoltre, il punto H, comma 3, art. 28 del GDPR: le **ispezioni** presso i responsabili (esterni) del trattamento. Anche questo è un **momento difficile**, che costringe il titolare a concordare con il fornitore di servizi (per esempio, la ditta che si occupa dell'archiviazione storica della documentazione cartacea) tempi e modalità di verifica. Bisogna far comprendere al fornitore che **non è un segnale di mancanza di fiducia**, magari consolidatasi in anni di proficua collaborazione, ma un elemento al quale, in passato, non era stata dedicata l'attenzione necessaria e che, per il futuro, può servire a migliorare il lavoro di tutti.

Le **verifiche** (o gli audit, come è più corretto chiamarli) **non chiudono definitivamente il cerchio**: spesso lo riaprono per riprendere l'analisi e, se necessario, agire con ulteriori misure tecniche ed organizzative.

Il faticoso ma affascinante lavoro del consulente privacy non finisce mai.

Articolo a cura di **Giuseppe Diretto** e **Francesco Maldera**