Tutela dei dati personali: tornare ai fondamentali - Parte II

Author : Stefano Gorla

Date : 22 Maggio 2020

Vorremmo ribadire i concetti esposti nel precedente articolo, dato il prolificare di informazioni non sempre corrette e di "super esperti" in tema tutela dei dati personali: lo faremo attraverso dei semplici esempi in modo da poter essere i più chiari possibile.

Ringraziamo, già ora, chi avrà la costanza e la pazienza di leggere questo articolo fino alla fine.

L'approccio al **trattamento dei dati personali** e alla loro tutela, generalmente, non segue un percorso scientifico ma è lasciato alla "buona volontà" delle persone e, molte volte, al caso.

Il metodo scientifico, proposto da Galilei, prevede che sia formulata un'ipotesi, magari derivante da un'osservazione, da una sperimentazione, una verifica attraverso dei modelli magari matematici, cioè una correlazione, e una conferma o disconferma dell'ipotesi con la ripetibilità dell'esperimento per dare universalità alla soluzione.

Molti partono con il trattamento dei dati personali "al contrario". Sviluppo di un'app (oggi molto attuale), sviluppo di un software oppure nuovi trattamenti e poi verificano se questi dati sono tutelati. Se questo non succede si corre ai ripari... ma dopo! Per fortuna **il GDPR ha introdotto l'art. 25**, ancor oggi sconosciuto e poco applicato.

È una questione di metodo. Gli antichi pastori ammucchiavano una pietra per ogni pecora che usciva dall'ovile e le toglievano per ogni pecora che rientrava nell'ovile. Non sapevano che stavano facendo un'operazione matematica semplice (addizione) e che stavano contando. Controllavano se le pecore erano tutte presenti. Allo stesso risultato si può arrivare considerando un numero - 1 - e addizionandolo, attraverso un operatore matematico (+), a se stesso tante volte. Si ottiene lo stesso numero: solo che alla base ci sono le regole della matematica che ci permettono di capire cosa succede. Il numero uno è primo dispari, è neutro nella moltiplicazione e nella divisione appartiene ai numeri naturali, etc. L'approccio è diverso.

Riportiamo ora **un piccolo esempio.**

Vogliamo costruire una barca per attraversare un lago. Alcuni prendono il materiale costruiscono la barca la varano e affonda. Allora ne costruiscono un'altra modificata la quale

affonda lo stesso. Per approssimazioni successive e varie modifiche riescono alla fine a farla galleggiare. Ma quante ne abbiamo affondate!

Invece il metodo scientifico parte dalla teoria già nota, il principio di Archimede, che spiega il fenomeno considerando alcune variabili quali la massa M, la densità dell'acqua ?, la densità del materiale $?_1$, il volume V, il peso P, il peso specifico p, che vengono correlate utilizzando delle formule per calcolare il galleggiamento. Non solo ma è necessario considerare il contesto: il lago è composto da acqua salata o acqua dolce? La barca è a motore o a vela? Quale è lo scenario? (Tornando ai numeri, parliamo di numeri naturali o complessi?).

Lo stesso vale per la **privacy**/tutela del dato personale.

Quindi, date le regole - gli artt. 7 e 8 della carta dei diritti fondamentali della costituzione europea e l'art. 2 della Costituzione - bisogna considerare le variabili: liceità, necessità, proporzionalità, necessità, pertinenza, non eccedenza e base giuridica. Bisogna verificare il contesto e gli scenari presenti (dove faccio il trattamento, tipologia dei dati, tipologia di azienda, tipologia di interessati, etc.)

Queste variabili sono poi correlate attraverso delle equazioni (informative, lettere di nomina, consensi, adozione delle misure di sicurezza, analisi dei rischi, etc) supportate dalla teoria (nell'esempio, il GDPR).

Risulta allora chiaro che è necessario un approccio più scientifico per implementare un sistema forte e affidabile che garantisca il rispetto dei requisiti e la dimostrazione (come per il metodo di Galileo), o *accountability*, che quanto posto in essere sia applicato ed efficace.

Come abbiamo sottolineato sia in questo articolo che nel precedente, viviamo in un periodo dove, soprattutto grazie al web, "tutti sanno tutto di tutti". È così che ci piace riprendere un aforisma di uno dei più grandi filosofi greci, che in tempi non sospetti sosteneva che *"il vero sapiente è colui che sa di non sapere".*

Pertanto, solamente nel momento in cui realizziamo e prendiamo coscienza del fatto che per potere prendere determinate decisioni dobbiamo anche avere gli strumenti adatti per farlo, possiamo asserire di essere in grado di governare gli eventi.
Il nostro paradigma risulta essere: situazione da affrontare >>> valutazione degli strumenti in mio possesso >>> approfondimento e arricchimento delle conoscenze tematiche >>> scelta delle decisioni >>> possibilità di governare un processo.

In tutto ciò non dobbiamo dimenticare il ruolo che l'**ipengiofobia** esercita su tutti noi. Probabilmente, molti dei lettori non sanno cosa sia l'ipengiofobia ma il solo fatto che contenga "fobia" fa venire in mente la paura di un qualcosa. Tal Katz-Navon è Professoressa Associata di Comportamento Organizzativo presso la Arison School of Business del Centro Interdisciplinare (IDC) Herzliya, Israele. La prof.ssa Katz-Navon studia i modelli organizzativi, la motivazione dei dipendenti, i processi di apprendimento, l'autonomia e la voce, che mirano a migliorare i dipendenti e le prestazioni organizzative. In un suo studio, analizzò il livello di dettaglio delle regole di 47 dipartimenti sanitari di diversi ospedali israeliani. Nello specifico vennero raccolti i

dati in merito al numero di incidenti che avvenivano ogni anno durante le operazioni e altri trattamenti. L'obiettivo era di mettere in relazione il numero e il dettaglio delle regole con il numero e la gravità degli incidenti. La prof. Tal Katz-Navon osservò che nei dipartimenti con poche regole era stata rilevata una media di 13 incidenti all'anno, media che cresceva parallelamente al numero di regole a cui il personale doveva attenersi in ogni struttura oggetto dell'indagine. La particolarità che emerse dallo studio, fu che la **relazione tra regole e incidenti** non era lineare bensì curvilinea, con una tendenza esponenziale.
L'ipengiofobia rappresenta pertanto la paura delle regole!

Le regole producono **certezze**, ma troppe regole producono **incertezze**; e quando ci sono troppe regole, le persone cominciano ad aver paura di infrangerle. Le persone cominciano ad essere ossessionate e queste diventano l'unico obiettivo su cui ci si concentra. *Cogito ergo sum*, **le persone smettono di pensare.**

Valutare e gestire il rischio (cioè diminuire la probabilità che l'errore umano ma non solo possa avverarsi) è senza dubbio di fondamentale importanza. Ma è un'attività che si realizza introducendo controlli sui processi e standard di comportamento (procedure, regole di condotta) per le persone.
E purtroppo esiste un limite alla possibilità di introdurre regole e controlli all'interno delle organizzazioni:

- troppi controlli rallentano l'esecuzione dei processi ed incidono negativamente sulla performance organizzativa,
- troppe regole finiscono per immobilizzare la capacità decisionale delle persone (ipengiofobia).

Sostenere che si possa realizzare un sistema perfetto è un azzardo, in quanto non esiste il sistema perfetto, vale a dire quello in grado di azzerare un rischio. Il principio previsto dall'**art. 25 del GDPR** - protezione dei dati fin dalla progettazione e protezione per impostazione predefinita – è in parte uno strumento di lavoro nuovo; la bibliografia di riferimento è ancora troppo scarna e, soprattutto, per lo più priva di esempi applicati e affidabili. Il controllo totale delle persone e dei processi finirebbe per annientare le persone e l'organizzazione, motivo per cui risulta fondamentale tracciare un percorso che rispecchi fin dalla sua progettazione quella che sarà la sua operatività.

Tutti noi sappiamo che nessun sistema di protezione da attacchi cibernetici al mondo è in grado di escludere una violazione dei dati personali che le aziende gestiscono, indipendentemente dalle risorse che vengono investite sia da un punto di vista delle persone che economico. Le aziende devono garantire che la gestione dei procedimenti e l'erogazione di servizi che coinvolgono dati personali avvengano nel pieno rispetto delle regole.

Vediamo pertanto quali possono essere queste **poche ma fondamentali regole** a cui proponiamo di fare riferimento e di non dimenticare in fase di progettazione e impostazione:

- Quali dati tratto?
- Per quanto tempo e dove li conservo?

- Perché e per quali fini conservo e tratto i dati?
- È stata identificata la base giuridica per trattare i dati?
- Chi ha accesso all’interno della mia azienda, e con quali modalità, a questi dati?
- Sono stati identificati gli strumenti utilizzati per trattare i dati?
- Vengono coinvolte parti terze (in caso affermativo, bisogna rivedere tutti i punti sopra esposti)?
- Quale è il ruolo dei soggetti nel trattamento di dati?
- Quali sono i rischi corrono le persone di cui tratto i dati a seguito dei miei trattamenti?
- Ho valutato quali possono essere le violazioni dei dati?
- Mi sono sincerato che siano state prese particolari precauzioni per un eventuale trattamento dei dati *ex* art. 9 del GDPR?
- Ho una mappatura del flusso dei dati?
- Il trattamento necessita di implementare l’architettura informatica attualmente in essere in azienda?
- C’è corresponsione di informazioni tra le informative in essere *ex* art. 13 e 14 del GDPR e il nuovo trattamento dei dati? Questa documentazione deve essere aggiornata?

Conclusioni

Bisogna tenere in considerazione i fattori che incrementano il rischio di violazione dei dati (come ad esempio una scarsa chiarezza delle regole, carenza di personale, mancanza di procedure, assenza di rotazione, rilevanza economica, complessità delle operazioni da svolgere, ecc...), per cercare di limitare il danno di una eventuale violazione pur sapendo che questi rendono vulnerabili i processi. La **consapevolezza** nei processi lavorativi richiamata nel primo articolo deve essere introdotta nella fase progettuale di un nuovo trattamento dei dati, ancor prima di richiederla all’interessato finale.

Volendo riassumere e sintetizzare quanto esposto, possiamo dire che la valutazione del rischio, in combinazione con la qualità e alla consapevolezza del trattamento, devono essere oggetto di un'attenta analisi dei processi. Gli interessi in gioco sono molti e un'accurata analisi degli inneschi interni ed esterni, basati sulle relazioni che "supportano", contribuisce a redigere poche ma essenziali e chiare regole a cui attenersi.

Articolo a cura di **Stefano Gorla** e **Augusto Bernardi**