

La tutela dei dati personali attraverso strumenti di *diritto morbido* (*soft law*)

Premessa

“Viviamo ormai in una *law-saturated society*, in una società strapiena di diritto, di regole giuridiche dalle provenienze più diverse”¹ Lo stesso Rodotà (quando ancora indossava le vesti di Presidente dell’Autorità garante per la tutela dei dati personali) sottolineò l’inarrestabile moltiplicarsi di fenomeni di redistribuzione dei poteri normativi durante una Riunione interistituzionale sulla legislazione presso l’Organo Parlamentare competente². In tale sede individuò almeno otto livelli di fonti normative: accordi internazionali, atti dell’Unione europea, legislazione nazionale, legislazione regionale, regolamenti e varie fonti di decretazione, **codici di autoregolamentazione, standard internazionali e standard tecnici**.

Le ultime tre categorie rientrano in quello che viene definito *diritto morbido* (*soft law*), un **sistema normativo che congiunge e completa i sistemi normativi classici**. Il *diritto morbido* comprende infatti un complesso di fonti di natura *atipica* che le istituzioni statali, comunitarie e internazionali hanno iniziato ad impiegare in un momento storico contrassegnato dalla cronica carenza dimostrata dagli strumenti tipici di produzione giuridica. Se è pur vero che il persistente ricorso alle autoregolamentazioni può essere visto come un mezzo per sottrarre al Parlamento la propria potestà legislativa, nel campo della tutela dei dati personali il *diritto morbido* rappresenta una buona opportunità per cercare di controllare l’inarrestabile accelerazione indotta a livello mondiale dal progresso scientifico e tecnologico in atto. La globalizzazione economica, oltrepassando i confini nazionali, rende progressivamente più critica la tradizionale dimensione spazio-temporale con la quale i popoli sono sempre stati abituati a confrontarsi. Questo fenomeno è ancora più evidente se si esamina l’ambito concernente la tutela dei dati personali abbinato all’utilizzo della rete internet, che di fatto annulla qualsiasi tipo di frontiera.

Linee guida

Dal punto di vista nazionale nell’anno in corso si segnala l’approvazione da parte dell’Autorità di protezione dei dati di Linee guida in materia di "**Rapporto di lavoro in ambito pubblico**", "**Rapporti con la clientela in ambito bancario**", "**Pubblicazione e diffusione di atti e documenti di enti locali**", "**Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero**" e da ultimo "**Trattamento dati nell’ambito delle sperimentazioni cliniche di medicinali**" che seguono quelle pubblicate diversi mesi fa titolate "**Guida pratica e misure di semplificazione per le piccole imprese**", "**Linea guida sul rapporto di lavoro privato**", "**Linee Guida sull’utilizzo di Internet e della Posta elettronica**". Soprattutto quest’ultime hanno introdotto il concetto di "*Policy aziendali*" (mutuato da paesi di matrice anglosassone in cui risulta molto in voga in entità di una certa dimensione), che solo apparentemente risulta estraneo al nostro ordinamento. A ben vedere infatti sia l’Art. 12 che l’art. 111 D.Lgs. 196/03 (Codici di deontologia e di buona condotta) evidenzino come il rispetto delle disposizioni contenute in tali codici costituiscono condizione essenziale per la liceità e correttezza del trattamento dei dati personali. Senza peraltro dimenticare le norme che in via generale regolamentano le obbligazioni ed i contratti nel codice civile (Art. 1175 “Comportamento secondo correttezza” e Art. 1375 “Esecuzione di buona fede”) e le norme specificamente riferite al rapporto di lavoro (Art. 2104 “Diligenza del prestatore di lavoro” e Art. 2106 “Sanzioni disciplinari” e L. 300/70 recante lo Statuto dei lavoratori, su tutti). Particolarmente attuale è infine la responsabilità “amministrativa” delle persone giuridiche prescritta

¹ S. Rodotà, La Vita e le Regole. Tra diritto e non diritto.

² <http://leg13.camera.it/organiparlamentarism/247/14106/15586/15639/documentotesto.asp> (sito consultato, e documentato verificato il 25 settembre 2008)

dal D.Lgs. 231/01. Seppure quindi dall'onere di elaborare “*Policy aziendali*” (*diritto morbido*) non discenda una norma prescrittiva sanzionatoria specifica in caso di mancata applicazione da parte del datore di lavoro, si devono comunque valutare i singoli aspetti considerati dal “mosaico” di riferimenti normativi sopra elencati, da cui scaturiscono precise responsabilità giuridiche. Anche l'attuale Presidente dell'Autorità Garante, Francesco Pizzetti, ha dichiarato durante il discorso di presentazione della Relazione 2007³ che l'obiettivo delle Linee guida è quello di **fornire una risposta ai principali interrogativi di ciascun settore favorendo le pratiche virtuose** e segnalando gli errori più frequenti sottolineando la predilezione di un approccio preventivo piuttosto che sanzionatorio.

Standard Internazionali

Uscendo dall'ambito nazionale, dopo un prolungato periodo di diffidenza, si sta estendendo l'esigenza di adottare degli standard riconosciuti a livello internazionale. Non è pertanto da condividere l'interpretazione di quanti escludono dal novero del *diritto morbido* gli strumenti d'elaborazione di standard o di redazione di codici di pratica, ma al contrario si ritiene appropriato segnalare l'importanza e l'influenza nei rapporti di forza tra gli operatori economici che giocano gli organismi come l'ISO. L'ISO, ovvero l'organizzazione internazionale di normazione, nasce con la finalità di fornire delle **norme non giuridiche** che, stabilendo degli standard riconosciuti a livello internazionale, inducano le organizzazioni al **miglioramento continuo** consentendo a queste di rispondere in maniera appropriata alle sfide dei nostri anni e di quelli a venire: sicurezza e globalizzazione, rischi e nuove tecnologie. Oggi le norme ISO sono riconosciute in ben 157 Paesi. Tra la normazione tecnica e la legislazione esiste peraltro un rapporto stretto e complesso. Se infatti l'applicazione delle norme tecniche non è di regola obbligatoria (*diritto morbido*), quando queste vengono richiamate nei provvedimenti legislativi può intervenire un livello di coerenza, delimitato pur sempre al contesto di riferimento. A tal fine è possibile effettuare una ricerca all'interno delle banche dati sul sito dell'Ente Nazionale Italiano di Unificazione (consultazioni possibili rispettivamente sulla Gazzetta Ufficiale dell'Unione Europea⁴ e sulla Gazzetta Ufficiale della Repubblica Italiana⁵).

Anche i Garanti del mondo sono alla ricerca di regole comuni: tra le risoluzioni approvate a **Montreal** nel **settembre 2007** in occasione della 29esima “*International Conference of Data Protection and Privacy Commissioners*” si segnala anche quella sulla **necessità di tradurre in standard tecnologici i principi di protezione dei dati**⁶. “La seconda risoluzione affronta il problema della definizione di standard universali in materia di *Privacy* in collaborazione con l'ISO (l'organismo internazionale che si occupa di fissare standard tecnologici e di processo). Il tentativo di tradurre i principi di protezione dati in regole tecnologicamente efficaci merita di essere sostenuto, anche se attualmente in ambito ISO ciò avviene con riguardo soprattutto alle tematiche della sicurezza dei sistemi informativi più che alle metodologie per garantire il rispetto della *Privacy*. La Conferenza di Montreal invita tutte le Autorità di protezione dati a partecipare attivamente al processo di definizione di tali standard anche attraverso un migliore coordinamento delle iniziative nazionali ed il coinvolgimento diffuso del mondo scientifico e della ricerca”⁷.

In Italia lo standard **ISO/IEC 27001:2005**, relativo ai *Sistemi di gestione per la Sicurezza delle Informazioni*, sta contribuendo allo sviluppo ed alla diffusione della cultura della sicurezza in un contesto certamente non facile. Il numero di società accreditate è relativamente basso (si contano circa 150 aziende certificate⁸) anche se si attendono sviluppi futuri significativi. Ciò sottolinea il problema della consapevolezza delle organizzazioni in ordine alla *security*, come elemento rafforzante nel sistema di

³ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1533086> (sito consultato, e documentato verificato il 25 settembre 2008)

⁴ <http://catalogo.uni.com/gazzette/guue.html> (sito consultato, e documentato verificato il 25 settembre 2008)

⁵ <http://catalogo.uni.com/gazzette/guri.html> (sito consultato, e documentato verificato il 25 settembre 2008)

⁶ http://www.privacyconference2007.gc.ca/Terra_Incognita_home_E.html (sito consultato, e documentato verificato il 25 settembre 2008)

⁷ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1448246> (sito consultato, e documentato verificato il 25 settembre 2008)

⁸ Fonte Sincert: <http://www.sincert.it/RisultatiRicerche.asp?id=260&root=elenchi> (sito consultato, e documentato verificato il 25 settembre 2008)

gestione dei rischi aziendali. Non è ancora adeguatamente percepito dal *management* come strategico per il corretto funzionamento del *business* aziendale ma anzi viene percepito come un costo piuttosto che come una risorsa da sfruttare come vantaggio competitivo. Lo standard si focalizza sui requisiti di riservatezza, integrità e disponibilità dei dati e sebbene non sia direttamente riferito alla *Privacy* è possibile “mappare” nelle numerose contromisure previste dallo standard tutti i requisiti rilevanti normati del D.Lgs. 196/03 e dal disciplinare tecnico allegato (Misure di sicurezza fisiche, logiche ed organizzative) ottenendo una *Compliance* gestibile soprattutto per organizzazioni particolarmente complesse.

Tra gli standard ISO con focus specifico sulla *Privacy* attualmente pubblicato (60/60) si segnala l'**ISO 22307:2008 Financial services - Privacy impact assessment** che riconosce come una valutazione d'impatto sulla *privacy* è uno strumento di gestione importante per i servizi finanziari e bancari per individuare e attenuare le questioni della *privacy* e dei rischi connessi con l'elaborazione automatizzata dei dati dei consumatori.

Al momento in “fase di richiesta” (40/60) è l'**ISO/DIS 24100 Privacy - The basic principles for probe personal data protection** che individua i principi di base di protezione dei dati personali (terminologie principi e caratteristiche comuni, descrizione degli aspetti relativi alla *Privacy* contenuti nelle Linee guida di sicurezza)

Sono in fase preparatoria (20/60) l'**ISO/IEC WD 29100 A Privacy framework** che definisce i requisiti posti a salvaguardia della *Privacy* in relazione ai processi dei sistemi ITC e l'**ISO/IEC WD 29101 A Privacy reference architecture** che descrive le migliori pratiche da adottare per l'implementazione dei requisiti tecnici richiesti dalla *Privacy* in relazione alle architetture dei sistemi ITC (definizione delle varie fasi del ciclo di vita nella gestione dei dati, definizione di ruoli e responsabilità di tutte le parti interessate, presentazione di un target di architettura, definizione di una guida per la pianificazione e la costruzione di architetture di sistema, strumenti di facilitazione per il corretto trattamento dei dati attraverso le piattaforme di sistema).

Conclusioni

Sostanzialmente il dinamico incremento a cui si assiste di strumenti alternativi alle fonti tradizionali è determinato dalla funzione estremamente positiva che essi svolgono. Il *diritto morbido* attraverso Linee Guida e Standard Internazionali può indubbiamente originare l'aspettativa che la condotta di Stati, organizzazioni internazionali ed i singoli si conformeranno alle regole di condotta, seppure non ancora vincolanti, in essi contenuti. Per mezzo del *diritto morbido* è possibile ricorrere a processi regolativi determinati, soprattutto nei settori economici, in cui i vari attori in gioco intendono porsi obiettivi comuni. In tal senso il *soft law* anticipa le conseguenze di obblighi futuri e può essere impiegato come base di partenza (attraverso la costituzione di tavoli di discussione che ne definiscano i “contorni” legislativi) per elaborare successivamente norme nazionali cogenti. Si percepisce l'esigenza di fonti di diritto non calate dall'alto, ma piuttosto di modalità giuridiche innovative che troveranno sempre più spazi di intervento in futuro, soprattutto in tematiche legate al trattamento dei dati personali.

Parma, 25 settembre 2008

Dott. Alessandro Rodolfi
Fellow IIP