Università Commerciale
Luigi Bocconi

La tecnica del consenso nell'era dei *big data*: Verso una tutela dinamica ed un controllo decentralizzato dei dati personali?

Aura Bertoni

E-Privacy 2013, Winter Edition – Milano, 15-16 novembre 2013

L'approccio europeo alla protezione dei dati personali

- La protezione dei dati personali (DP) è un'innovazione giuridica di origine europea che sta gradualmente, con alterni consensi e sorti, estendendosi a paesi terzi
- La protezione dei DP si riferisce alla tutela attraverso la regolazione giuridica delle informazioni personali relativa a persona fisica, identificata o identificabile
- Nasce come **aspetto complementare** alla tutela della privacy e si sviluppa come **diritto autonomo,** non soltanto nel quadro delle trasposizioni nazionali delle direttive europee ma altresì nelle carte costituzionali dei paesi membri dell'UE
- L'articolo 16 del Trattato di Lisbona gli attribuisce il carattere di 'disposizione di carattere generale' e gli articoli 7 e 8 della Carta dei diritti fondamentali dell' UE considerano **il rispetto della privacy e la protezione dei dati personali diritti fondamentali strettamente correlati ma distinti**
- Il riconoscimento della tutela dei DP a livello di **fonti primarie** esplicita l' approccio europeo fondato sui diritti fondamentali dell' uomo (quindi, ad esempio, non può essere non oggetto di scambio a fronte di **benefici economici**)

Il riconoscimento giuridico del consenso nella normativa UE

•L'art. 8, comma 2, della Carta dei diritti fondamentali dell'UE stabilisce che i "dati [personali] devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al **consenso** della persona interessata o a un **altro fondamento legittimo** previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica"

↓

–Benché vi siano diversi, specifici, fondamenti giuridici per il trattamento dei dati personali, l'articolo 8 attribuisce espressamente una **funzione cardine al consenso**

–Soltanto il trattamento dei DP senza consenso (ad es. dati necessari per adempiere agli obblighi derivanti da un contratto) è sottoposto ad un test di necessità

–Tuttavia il consenso lascia intatti i principi relativi alla qualità dei dati: principio della buona fede, principio di **finalizzazione;** principio di **necessità o pertinenza**; principio di correttezza; principio della conservazione/durata

Nozione e uso del consenso in materia di DP

•Il **consenso** è lo strumento per esercitare il **controllo** sui dati personali quando il trattamento non è autorizzato dalla legge in quanto necessario

•La disciplina del consenso regola, pertanto, le modalità di esercizio del controllo

•Le modalità di esercizio riflettono alcuni fondamentali valori insiti nelle democrazie moderne:

- il diritto individuale all'auto-determinazione informativa e alla libera costruzione della personalità
- l'interesse sovra-individuale ad una società plurale dove valori, ideali e preferenze non si conformino al volere della maggioranza o degli interessi di mercato

↓

•Difficoltà nell'esercizio di un **controllo effettivo…**

- La tecnica del consenso (e del rifiuto) di fornire i propri DP si rivela un esercizio vuoto a fronte di un linguaggio ambiguo e complesso
- Gli interessati sono sempre più "vittime consapevoli" che danno il consenso per non essere esclusi dalla sfera pubblica e quindi da un numero crescente di processi sociali, conoscenze, beni e servizi…
- … (segue)

…l'impatto di *big data* e *data mining* sullo strumento del consenso è considerevole

→ Il titolare del trattamento non conosce in anticipo le potenziali correlazioni, ossia le **finalità** del trattamento

- pertanto non può fornire un'**adeguata informativa** all'interessato
- pertanto l'interessato non può fornire un **consenso effettivo**

→ L'obbligo del consenso non si applica al trattamento di quei **dati non personali** che permettono le correlazioni e l'estrazione di **informazioni personali**

↓

–Come consentire l'esercizio del consenso/rifiuto nell'era dei ***big data?***

–La pura **tecnica del consenso rifiuto** di fornire i propri dati personali rappresenta un'adeguata risposta al fenomeno dei ***big data?***

→ Proposta: ristabilendo la centralità della persona/interessato, in qualità:

- soggetto debole nel trattamento dei DP (parte maggiormente meritevole di tutela)
- soggetto attivo (vs consumatore passivo)

↓

evidente contraddizione o attuabile combinazione?

paternalismo vs liberalismo?

↓

- persona/interessato è ancora prima status sociale che categoria giuridica
- lo **status** di interessato è statico (e debole) ma il suo **ruolo** nel trattamento è dinamico (e 'attivabile')

1. riconoscere il suo **status di soggetto debole:**
   - significa ammettere la diversa posizione di partenza dei soggetti coinvolti nel trattamento
   - significa riconoscere la potenziale emersione di distorsioni all'interno di un contesto dove la «offerta» è più debole della «domanda» (pur non essendo formalmente un mercato)
2. 'attivare' il suo **ruolo di soggetto attivo**
   - significa superare l'asimmetria di potere attribuendogli maggior potere (concreto)
   - significa virare verso *(i)* una tutela dinamica dei dati personali e *(ii)* il controllo decentralizzato dei dati

1. Tutelare il suo **status di soggetto debole: come?**

Applicando il principio privacy by default e by design attraverso l'introduzione nella normativa di regole di default che permettano il riequilibrio di potere (ad esempio, esplicitando che il rifiuto dell'interessato non permette discriminazioni del responsabile del trattamento nel quadro di sottostanti transazioni)

2. 'Attivare' il suo **ruolo di soggetto attivo: come?**

(i) Tutela dinamica dei dati

- riconsiderazione dell'**ambito di tutela**: *big data* e informazione concernente una persona identificabile attraverso incrocio di dati non-personali (es. de-anonimizzazione; de-individualizzazione della persona e profilazione di gruppo)
- **innovazione tecnologica** per il trattamento dei *big data* incentrata su modelli di *metadata tagging* che impediscano la re-identificazione
- adozione del modello di **consenso dinamico** (www.encore-project.info), tra l'altro già sperimentato nel contesto delle banche biologiche, liberando da tutela dalla rigidità dell'attuale carattere dicotomico del consenso (sì/no; on/off) che espone a rischi di inclusione ed esclusione dai *big data*

(ii) Controllo decentralizzato dei dati

- emancipazione della persona/interessato nell'esercizio del diritto alla tutela dei dati che la riguardano ("no engagement without empowerment")
- **informativa** che espliciti il "valore d'uso" dei dati in quel contesto di trattamento e che permetta l'esercizio del consenso/rifiuto al mutare del contesto grazie a rinnovati **supporti tecnologici** (vedasi 'privacy rights management' system)
- contribuire di riflesso alla diffusione delle potenzialità innovative dei big data