LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Scienze giuridiche
CERADI – Centro di ricerca per il diritto d'impresa

"Cooperative Commons" From Privacy by Consent to Privacy by Contract

Alfonso Papa Malatesta

Luglio 2013

Roma, Luiss Guido Carli – May 13/14- 2013

"Cooperative Commons"

From Privacy by Consent to Privacy by Contract

- **Alfonso Papa Malatesta**

* * *

Buongiorno. Il tema di cui mi occupo nell'ambito della ricerca sui Cooperative Commons portata avanti dal Dipartimento di Scienze Politiche della Luiss attiene al trattamento dei dati personali. In particolare al trattamento dei dati che gli utenti, ognuno di noi, rilascia in rete.

L'utilizzo di internet implica il trattamento di informazioni digitalizzate, molte delle quali rientrano nella definizione giuridica di "dati personali". Il Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003), di derivazione comunitaria, indica cosa debba intendersi per "dato personale". E' una definizione oramai familiare per i giuristi. Riguarda ogni "informazione" relativa ad una persone fisica, che permetta di identificarla, anche indirettamente. Secondo la legge ogni informazione, anche di per sé non identificante, è un "dato personale" se attraverso quella informazione è possibile risalire ad un'altra o più altre informazioni che infine permettano di identificare la persona in questione. Ecco la definizione contenuta nel Codice.

Oggi i dati personali evocano immediatamente la "privacy".

Pertanto la "protezione" dei dati personali richiama a sua volta ed immediatamente la "tutela" della privacy.

Va però rilevato che "privacy", in italiano assimilabile a "riservatezza", è termine utilizzato per molti scopi, molti dei quali vanno ben oltre la definizione di "dato personale" contenuta nella legge e le finalità dalla legge stessa.

Nel linguaggio comune il riferimento alla "privacy" può essere usato per indicare la "sfera di riservatezza personale", e quindi il limite oltre il quale è moralmente sbagliato, secondo il comune sentire, intromettersi nella sfera di riservatezza altrui. Può essere utilizzato in relazione al diritto alla "privacy", cioè in relazione alle prerogative giuridicamente garantite di riservatezza delle

proprie azioni, ovvero agli obblighi che si è tenuti, sempre giuridicamente, a rispettare per non violare l'altrui diritto alla privacy. E' anche usato per indicare riassuntivamente una materia, un capo di indagine, oggetto di studio da parte di varie discipline (tra le quali il diritto).

Questa varietà di significati, ed il fatto che lo stesso contenuto giuridico della definizione di "privacy" abbia contorni piuttosto sfumati e incerti, provoca anche che "ragioni di privacy" siano spesso invocate come pretesto, cioè in modo non fondato su rigorosi presupposti giuridici, per negare l'accesso ai terzi ad una serie di informazioni detenute da soggetti pubblici e privati. Poiché tra i diritti degli individui, specie verso la pubblica amministrazione, v'è anche quello, non meno importante del diritto alla riservatezza, di accedere in determinati casi alle informazioni da essa detenute, si comprende come la tutela della privacy, specie quando non correttamente intesa e delimitata, sia destinata a generare conflitti tra interessi e finalità contrapposti.

Dico questo per rilevare come la terminologia d'uso comune si presti a notevoli confusioni. E come tale confusione si riverberi anche, quale fenomeno socialmente rilevabile, sulla consapevolezza dei singoli circa gli aspetti giuridici che riguardano la materia. Invero, tutela della "riservatezza" e protezione dei dati personali si muovono in ambiti giuridici distinti. I dati personali, ad esempio, sono protetti anche quando non hanno natura riservata: i dati personali contenuti in pubblici registri, quindi non riservati per definizione, restano comunque soggetti alla legislazione sul trattamento dei dati. In realtà, la legislazione in materia è in larga misura diretta a garantire il "controllo" degli individui sul trattamento dei propri dati piuttosto che la loro riservatezza.

Questo stato di cose non ha sinora aiutato il largo pubblico, e qui veniamo agli utenti di internet, a comprendere appieno il fenomeno dell'utilizzo dei dati che vengono disseminati e raccolti sulla rete, per essere elaborati, gestiti, conservati, trasmessi, ritrasmessi.

La scarsa consapevolezza del pubblico non aiuta il formarsi di istanze ragionate rivolte al legislatore ed ai governi, per la formazioni di leggi e di politiche in materia.

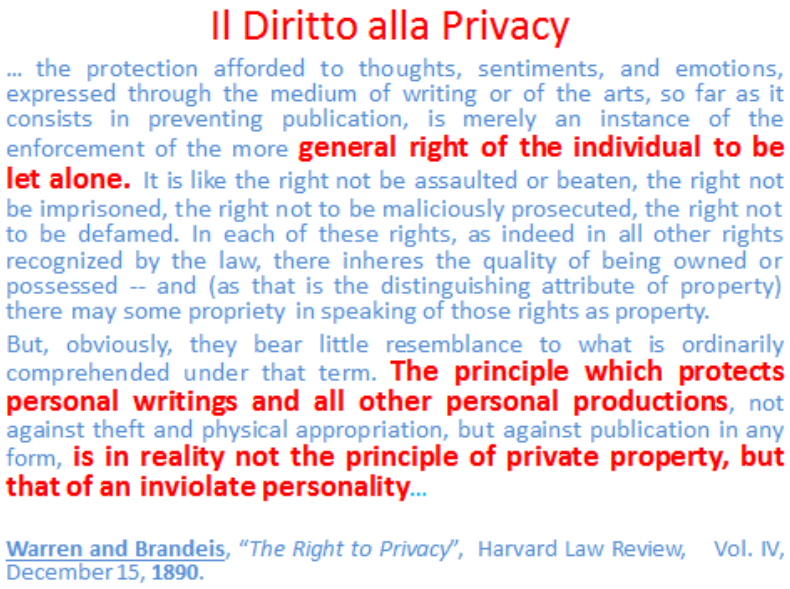
Voglio dire che il tema è discusso facendo appello ad una buona dose di emotività; senza che i termini del dibattito e le diverse implicazioni dell'intervento legislativo siano compresi a fondo, e senza che i diversi aspetti

che lo riguardano siano stati ben assimilati tra il largo pubblico e adeguatamente soppesati. Tra questi aspetti poco considerati, per quanto qui interessa, vi è anche quello relativo al "valore economico" dei dati, e quindi al valore che gli stessi hanno per chi li fornisce, da un lato, e per chi li raccoglie e li gestisce, dall'altro.

Ha così sinora prevalso un approccio strettamente "difensivo". In effetti, proprio gli aspetti relativi alla "protezione" della riservatezza personale sono i più chiari, i più nettamente avvertiti dal pubblico. E questo ha fatto sì che l'intervento legislativo si sia sinora appunto dedicato alla "tutela" degli individui, per quanto riguarda il trattamento dei loro dati, sulla base della descritta sovrapposizione tra protezione della "privacy" e protezione dei dati personali. Il tema giuridico (e di politica legislativa) all'ordine del giorno è e resta la "tutela" dei dati, considerata dai più come tutela della riservatezza.

E' l'istanza di "tutela" è stata più facilmente compresa e raccolta perché ha origini antiche, radicate appunto nella tutela della privacy. Già nella seconda metà del XIX secolo la tutela della riservatezza si è imposta come tema di intervento per il legislatore, sia in Francia che nei paesi di common law.

Negli Stati Uniti di America è ancora famoso l'articolo del 1890 a firma Warren e Brandeis che analizzava la questione della protezione dei propri sentimenti, della riservatezza, della propria immagine, rispetto alle invasioni altrui, specie da parte della libera stampa. Gli autori evidenziavano come l'appello all'inviolabilità del diritto di proprietà fosse naturale ma inappropriato, e introdussero il più avanzato concetto di diritto all'inviolabilità della sfera personale ("right to privacy").



Nel nostro sistema giuridico questo percorso, sulla scorta di teorizzazioni svolte soprattutto in Germania, ha condotto al riconoscimento del diritto alla riservatezza come un diritto della personalità. In Italia questo diritto è stato riconosciuto pienamente dalla giurisprudenza con un certo ritardo, negli anni '70.

Il diritto in questione, come si conviene alla categoria dei diritti della personalità (si pensi al diritto alla incolumità fisica), è assurto così al rango di diritto fondamentale, inviolabile, imprescrittibile. Diritto originario e assoluto, che cioè si acquisisce per il fatto d'esistere come esseri umani; che tutti devono rispettare e che si può far valere verso chiunque, senza necessità di preventivi accordi o contratti. E, come per i diritti della personalità, è indisponibile e non si prescrive, né vi si può rinunciare. I diritti della personalità non sono oggetto di scambio, non si possono cedere ad altri con un contratto. Sono spesso protetti dall'ordinamento a prescindere dalla, e anche contro la, volontà dell'individuo (che ad esempio volesse cedere il diritto all'incolumità fisica).

Privacy

- Diritto della personalità

Diritto fondamentale / Inviolabile

Assoluto (*erga omnes*)

Indisponibile (*autorizzazione revocabile*)

L'indisponibilità ha come corollario che nei rapporti con i terzi che possano incidere sull'oggetto tutelato dal diritto il consenso del titolare assuma la forma di una autorizzazione precaria. Se autorizzati dal titolare del diritto, i terzi possono lecitamente compiere atti che incidano sul bene giuridico protetto entro i limiti prestabiliti dall'ordinamento. Ma l'autorizzazione non trasferisce il diritto e le facoltà ad esso inerenti: il titolare potrà sempre revocare l'autorizzazione concessa al terzo, e ogni patto contrario sarebbe nullo.

Il carattere indisponibile dei diritti della personalità non esclude che le parti possano regolare alcuni riflessi patrimoniali collegati all'oggetto tutelato dai diritti della personalità. Il terzo autorizzato ad incidere sul bene tutelato dall'altrui diritto della personalità può convenire con il titolare di quest'ultimo la corresponsione di un vantaggio patrimoniale in suo favore.

Il profilo patrimoniale dei rapporti che riguardino l'autorizzazione del titolare di diritti della personalità è tra i più discussi nella dottrina giuridica. Non è facile conciliare una posizione giuridica che fa appello, in ultima analisi, a valori come la dignità umana, a valori morali irrinunciabili, con i riflessi prettamente patrimoniali inerenti il bene giuridico protetto. In alcuni casi, i giuristi e quindi il legislatore, hanno escogitato delle utili distinzioni logiche. Ad esempio, nel campo del diritto di autore, la dottrina latino-germanica ha tenuto distinto il diritto morale dell'autore, diritto della personalità indisponibile e irrinunciabile, dal diritto alla utilizzazione economica delle opere dell'autore. Il primo è un diritto della personalità non negoziabile, il secondo è un diritto di

carattere patrimoniale, e come tale possibile oggetto delle più disparate transazioni economiche. E' una esperienza da tenere presente nella nostra ricerca.

Tuttavia, queste distinzioni sono state il frutto di prolungate e controverse evoluzioni del pensiero giuridico, stimolato da pressanti ragioni di ordine pratico. In materia di dati personali il percorso è dunque ancora agli inizi. Per ora prevale, come detto, l'istanza "morale", la protezione della personalità dell'individuo. Gli aspetti patrimoniali sono stati poco indagati, anche perché l'opinione pubblica, come sopra rilevato, non li ha sinora ben individuati. Ad esempio, il valore economico che può assumere l'elaborazione dei dati è fenomeno ancora poco apprezzato, in quanto recente.

La prevalenza dell'esigenza di protezione giustifica il prevalere di uno specifico approccio alla questione, quello che nella nostra discussione, per semplificare, chiamerò "fear-based": l'approccio al problema del trattamento dei dati personali fondato sul timore di violazioni del diritto fondamentale in questione.

Non mi dilungo sul tema delle nuove frontiere nel trattamento dei dati personali aperte dall'avvento della tecnologia dei computer, del digitale e di internet. Le informazioni possono essere oggi trattate in modi impensabili sino a pochi decenni fa, grazie all'impiego dell'informatica e dei computer. Se a questo aggiungiamo il fatto che attraverso internet la raccolta e la circolazione delle informazioni hanno raggiunto livelli altrettanto imprevisti e giganteschi, si intuiscono sia la novità sia la vastità del fenomeno, di cui hanno già efficacemente parlato alcuni dei relatori che mi hanno preceduto.

Di fronte al nuovo fenomeno, la reazione fear-based è quella naturale, ed ha le sue indiscutibili buone ragioni. Qui di seguito mi limito a fare qualche distinzione, che mi sembra utile per il nostro discorso.

Un primo tipo di pericolo è ravvisato nell'utilizzo improprio dei nostri dati da parte di soggetti privati. Cioè le imprese, specie quelle multinazionali, globali, che attraverso internet raccolgono e gestiscono i nostri dati, per fini essenzialmente economico-commerciali. Agiscono a scopo di lucro, come si addice agli imprenditori sul mercato. Si temono abusi di vario genere, in danno di consumatori ed utenti.

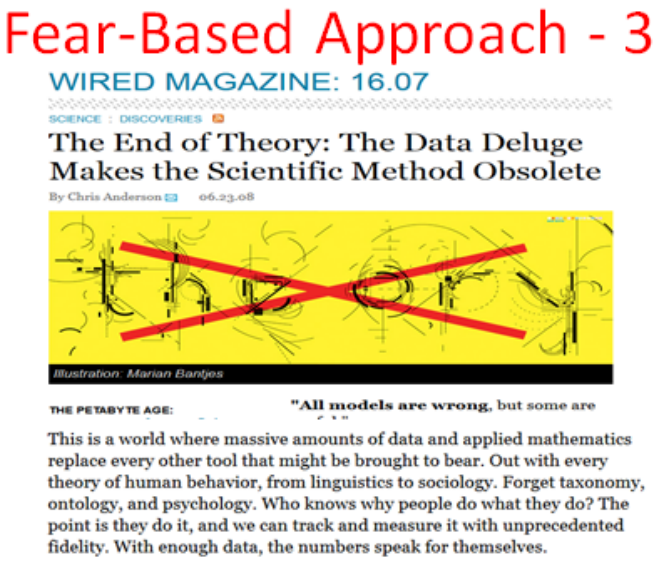
Fear-Based Approach - 1

Un secondo ordine di pericoli, quello che ad esempio negli Stati Uniti resta il più avvertito, riguarda l'utilizzo dei dati ed i possibili abusi da parte delle pubbliche autorità, da parte del governo. Il diritto alla riservatezza è minacciato dalle possibili intrusioni da parte di agenti governativi, che espongono gli individui a schedature, controlli ed a conseguenti ulteriori limitazioni delle libertà individuali, sino a minacciare le libertà politiche e quelle fondamentali.

Fear-Based Approach - 2

Un terzo tipo di timori, che concorrono a spiegare la reazione dell'ordinamento a difesa degli individui, attiene all'usuale paura che nutriamo

verso ciò che comprendiamo poco perché ancora troppo recente. E' la paura delle grandi novità e dell'ignoranza dei possibili sviluppi che potranno arrecare alle nostre consolidate visioni del mondo, ai modelli di vita e di relazione che ci sono familiari. Il timore dell'ignoto, insomma.



Come naturale, l'approccio fear-based ha provocato la reazione dell'ordinamento a difesa delle prerogative individuali.

La disciplina introdotta in materia dall'Unione Europea, a partire dal 1995, né è un buon esempio. Ed oggi la Commissione UE invoca una legislazione ancora più stringente a tutela dei nostri diritti.

Fear-Based Approach / Reaction

E il legislatore dell'Unione ha anche consacrato la tutela dei dati personali nella Carta dei diritti fondamentali, tra le altre libertà inviolabili dei cittadini europei.

Carta diritti fondamentali UE – Art. 8

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. **Tali dati 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.
3. Il rispetto di tali regole **è soggetto al controllo di un'autorità indipendente**.

E' interessante notare che l'approccio dell'Unione Europea, mentre garantisce la "protezione" dei dati, prende anche atto, da un lato, della ineluttabilità del loro trattamento e, d'altro lato, "costituzionalizza" l'istituzione di autorità amministrative (indipendenti dal potere esecutivo, dai governi) che presiedano alla concreta protezione degli individui. E' quest'ultima una visione

(a mio avviso paternalistica) tipica dell'approccio comunitario, che confida nell'istituzione dell'autorità indipendente come deus ex machina capace di risolvere i problemi più delicati, ove occorra neutralità di azione rispetto ai poteri politici.

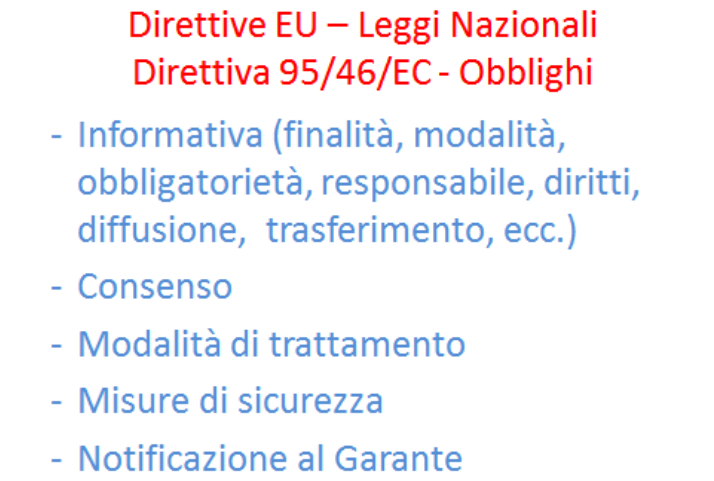
E' visione che peraltro non può che disinteressarsi del tutto dell'aspetto "economico" del trattamento dei dati, perché è rivolta a tutelare il diritto della personalità, privo di natura patrimoniale.

Sappiamo tuttavia come ai vari Garanti in giro per l'Europa siano stati attribuiti rilevanti poteri di normazione secondaria. Il loro intervento, le loro decisioni, hanno, ed avranno sempre di più, un forte impatto non solo per la garanzia del rispetto delle regole a tutela del diritto fondamentale, ma anche per la regolamentazione del settore economico che si va sviluppando intorno alla raccolta ed alla gestione dei dati. Il legislatore comunitario ha sinora mostrato di sottovalutare, non solo in questo campo, il problema dei difficili e contraddittori rapporti tra autorità indipendenti e poteri economici.

Comunque, quest'ultime riflessioni sono in parte estranee al nostro discorso, per il quale mi premeva piuttosto sottolineare come la legislazione in materia sia sinora orientata a definire il quadro a tutela dell'individuo, come richiesto dal fear-based approach. Ed è quindi una legislazione che rispecchia (ed al contempo alimenta) il dibattito corrente ed il comune sentire dei cittadini europei (non sfugga come la Commissione premetta, nell'annunciare la riforma della legislazione in materia, la rilevazione dell'Eurobarometro secondo cui il 70% dei cittadini è preoccupato da come vengono trattati i propri dati; sondaggio che avrebbe forse potuto stimolare anche qualche riflessione critica sull'efficacia dei Garanti e dell'approccio legislativo in vigore già da un paio di decenni).

La risposta del legislatore si è concretizzata nell'emanazione di direttive comunitarie e nel conseguente recepimento delle stesse all'interno degli ordinamenti nazionali.

Il nucleo fondamentale di questa legislazione, molto articolata, è rappresentato dall'introduzione del diritto dei singoli a "controllare" il modo in cui i propri dati vengono trattati da chi li raccoglie (i cd. data controllers, o "titolari del trattamento" nella nostra legislazione) e dall'obbligo di un trattamento rispettoso degli interessi dei singoli da parte dei data controllers. Il che si traduce, da un lato, nell'obbligo di fornire informazioni sulle modalità e finalità del trattamento da parte di chi gestisce i dati e, dall'altro lato, nel riconoscimento in favore degli interessati di una serie di facoltà, tra cui spiccano, ad esempio, quella di poter richiedere la rettifica dei dati e quella di richiedere la cancellazione degli stessi.



Una distinzione importante riguarda il trattamento dei dati da parte di pubbliche amministrazioni, le quali trattino i dati per adempiere le funzioni loro assegnate dall'ordinamento, e il trattamento da parte delle entità private, che agiscano per finalità economiche o comunque non nell'interesse generale.

Per il trattamento dei dati da parte dei soggetti privati occorre l'esplicita e preventiva autorizzazione da parte degli interessati. Il "consenso" al trattamento dei dati assurge così, nei rapporti tra privati, a momento qualificante nell'intero ciclo di vita del trattamento (dalla raccolta alla circolazione dei dati stessi). Nei rapporti tra i privati è l'autorizzazione del titolare, resa alle condizioni stabilite dalla legge, a rendere lecito il trattamento (salvo eccezioni, sulle quali non serve intrattenersi in questa sede).

Come anticipato, l'autorizzazione non è tuttavia all'origine di un contratto di diritto privato che riguardi il trattamento riservato ai dati. E' sempre revocabile. Abilita il terzo al trattamento, senza privare l'interessato delle proprie prerogative di controllo e revoca del consenso. Inoltre, seppure l'abilitazione al trattamento presuppone adeguata informazione circa le finalità, le modalità e i soggetti responsabili del trattamento stesso, non vincola il data controller all'effettivo svolgimento delle attività per le cui finalità ha richiesto l'utilizzo dei dati, né associa in alcun modo l'interessato alla gestione dei dati stessi nel traffico economico e giuridico. Segna i limiti dell'utilizzo consentito, ma il data controller non si obbliga a svolgere quel trattamento. Deve custodire i dati, e se li gestisce deve farlo nei limiti dell'autorizzazione e nei modi richiesti dalla legge, ma non è tenuto a rendicontarne l'utilizzo, specie in forma aggregata, e tantomeno a dare ragione delle operazioni (pur sempre nell'ambito di quelle preventivamente consentite) che egli stesso svolgerà (o non svolgerà) con i dati, ovvero delle transazioni (pur sempre nell'ambito di quelle preventivamente consentite) che avranno ad oggetto i dati stessi. Il valore economico procurato dalla gestione dei dati, ed i negozi giuridici che quel valore scambieranno sul mercato o all'interno dei processi aziendali del data controller, non formano oggetto del rapporto con il soggetto che ne ha consentito il trattamento. In breve, l'eventuale sfruttamento economico dei dati non è di per sé affare che coinvolga giuridicamente ed economicamente il soggetto a cui i dati si riferiscono e che presta il consenso al loro trattamento.

E il data controller autorizzato al trattamento può quindi dedicarsi alla gestione dei dati senza essere, sotto questo profilo e salvo il rispetto della legge e degli usi consentiti, in alcun modo vincolato ai soggetti che ne hanno

autorizzato l'utilizzo. Il data controller può orientarsi a trarre il maggior profitto possibile dalla lecita gestione dei dati.

Ed è questo, più in generale, l'altro possibile e diverso approccio alla gestione dei dati; quello basato sull'estrazione del valore associabile al loro trattamento, che chiamo qui per comodità value-based approach.

L'industria del trattamento, della fornitura dei dati, delle predizioni e delle metriche rese possibili dalla loro elaborazione (Big Data), è in pieno sviluppo. Per alcuni, è la vera new economy del prossimo futuro.

Dunque, un altro possibile approccio al trattamento dei dati è quello orientato alla evidenziazione delle potenzialità economiche collegate allo sfruttamento di questa risorsa, oggi più che mai reso possibile dalle nuove tecnologie e da internet.

Ciò vale nel settore della pubblica amministrazione, dove il trattamento può consentire risparmi e l'offerta di servizi pubblici più efficienti.

Value-Based Approach - PA

McKinsey&Company

Harnessing big data in the public sector has enormous potential, too. If US healthcare were to use big data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year. Two-thirds of that would be in the form of reducing US healthcare expenditure by about 8 percent. In the developed economies of Europe, government administrators could save more than €100 billion ($149 billion) in operational efficiency improvements alone by using big data, not including using big data to reduce fraud and errors and boost the collection of tax revenues. And users of services enabled by personal-location data could capture $600 billion in consumer surplus. The research offers seven key insights.

E vale ovviamente anche per il settore privato, dove già è vivo un ricco mercato di intermediari nella circolazione dei dati, come evidenzia ad esempio il caso della Acxiom, una società forse poco nota ma leader di un settore (database marketing) che movimenta miliardi di dollari.

Value-Based Approach: Acxiom

The New York Times

Mapping, and Sharing, the Consumer Genome

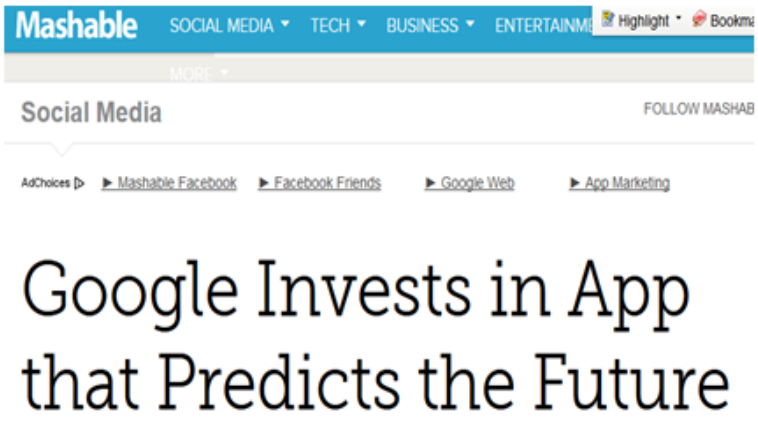
Justin Bolle for The New York Times

Acxiom's headquarters in Little Rock, Ark. Analysts say the company has amassed the world's largest commercial database on consumers.

By NATASHA SINGER
Published: June 16, 2012 | 92 Comments

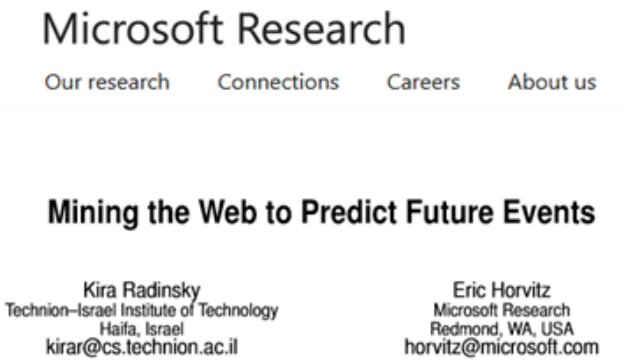
Le opportunità economiche offerte dal data-base marketing, dalla profilazione dei consumatori e degli utenti, dall'utilizzo delle informazioni raccolte per l'intelligenza delle strategie commerciali e aziendali, per la conquista di mercati e la più efficiente allocazione delle risorse investite, sono infinite e sono già oggetto di abbondante letteratura, così come di ingenti investimenti, specie da parte delle imprese dell'information economy.

Value-Based Approach / Predictions



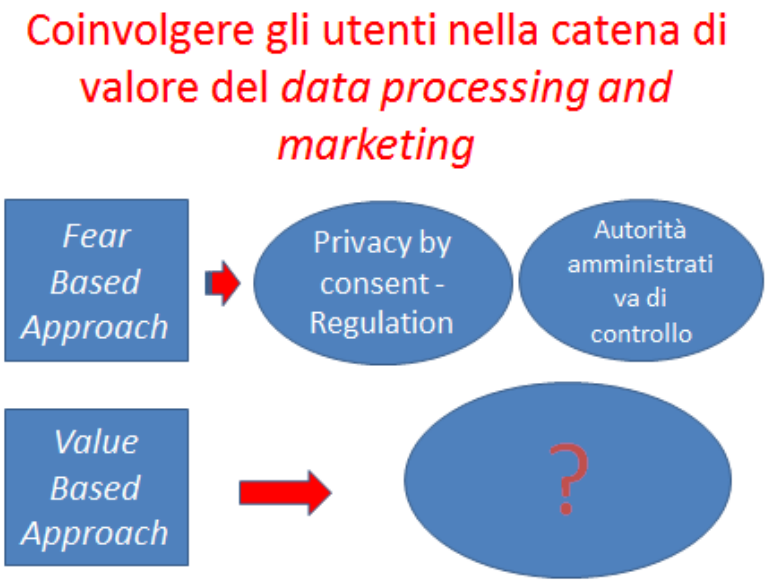
Contraltare del fear-based approach, la prospettiva in esame lascia intravedere utilizzi sempre più affascinanti, sino a quello dello sviluppo di tecniche per estrarre dal web la predizione di eventi futuri.

Value-Based Approach - Predictions



Quale è allora il ruolo dei singoli, coloro i cui dati sono raccolti ed utilizzati, nel contesto del value-based approach? Il fear-based approach ha offerto loro garanzie legislative, sino a sancire diritti fondamentali e la creazione di autorità amministrative indipendenti dedicate al controllo sul

trattamento dei loro dati. Ma quale è la posizione degli individui con riguardo allo sfruttamento economico di questa risorsa?



La ricerca sui "cooperative commons" portata avanti dalla Luiss vorrebbe indagare questo profilo, non solo per gli aspetti giuridici ed economici, ma allargando la prospettiva, innescando un dibattito culturale che vada oltre il fear-based approach per vedere coinvolti, in un ruolo più attivo, e non solo difensivo, gli individui, le persone, la collettività.

In effetti, le interazioni via internet, principale strumento per la raccolta dei dati personali, compongono un quadro in cui frammenti della nostra personalità sono continuamente oggetto di utilizzo da parte di terzi, senza nessun autentico coinvolgimento degli interessati. E' come se dietro le quinte della rappresentazione pubblica che ha luogo sui social network, su internet, si muovessero, un po' nell'ombra, altri attori e forze che non sono interessati affatto a quella rappresentazione, ma piuttosto impegnati freddamente a raccogliere ed elaborare le informazioni che ne derivano per sfruttarle ai propri esclusivi fini (economici, di governo, scientifici, ecc.).

Del resto, è naturale che sia in atto un profondo ripensamento del fenomeno, data la sua vastità, la velocità della sua evoluzione e il rilievo sociale ed economico che sta via via assumendo.

Lo scopo del progetto di ricerca è dunque quello di esplorare un approccio diverso da quelli sinora maggiormente indagati e che riguardano le istanze di tutela degli interessati.

Del resto, da più parti si è alla ricerca di nuovi modelli e risposte per regolamentare il settore.

Lo stesso modello europeo di difesa dei dati personali come garanzia delle libertà personali è messo in discussione dalla necessità di un bilanciamento con gli interessi del commercio e dell'industria: le imprese hanno bisogno di sfruttare i dati nella competizione globale, e le legislazioni troppo restrittive, o che determinano appesantimenti burocratici, o che frammentano il mercato europeo imponendo obblighi diversificati e costosi per il trattamento dei dati, rischiano di ostacolare la competitività delle imprese e la loro efficienza, in ultima analisi aumentando i costi anche a carico degli stessi consumatori ed utenti.

Sono state proposte altre opzioni, dando enfasi alla autoregolamentazione (specie in Nord America) o alla individuazione di standard per la tutela dei dati da integrare in via preventiva nell'ingegneria dei processi aziendali e dell'information technology (la cd. "privacy by design" di cui è fautrice la Dott.sa. Ann Cavoukian, in Canada).

Nei riguardi dei privati, si tratta di studiare in che modo il modello di "privacy by consent" adottato dalla legislazione europea possa essere integrato, attribuendo agli individui un qualche ruolo nella catena di valore generata dal data processing. Il che richiede di affiancare alla tutela morale del soggetto al

quale i dati si riferiscono, il riconoscimento di diritti e prerogative di carattere patrimoniale. Come detto, un precedente significativo lo si ritrova nel campo della proprietà intellettuale, nel diritto d'autore, per esempio.

Inoltre, nell'ambito dei rapporti giuridici a contenuto patrimoniale, la rappresentanza e gestione degli interessi dei singoli non sembra delegabile ad autorità pubbliche. In un'economia di mercato, il decentramento degli scambi dovrebbe restare alla base del modello di rapporti che si intenda normativamente strutturare. Per usare uno slogan, vorremmo studiare forme di "privacy by contract", facendo emergere una concezione che consideri i dati degli utenti come un "bene comune", proprio delle persone fisiche partecipanti alle interazioni via internet. Di qui, come vedremo a breve, l'idea dei cooperative commons.

Vorrei dare ora un esempio concreto del diverso possibile approccio, prendendo spunto da un'operazione molto comune, capitata credo a chiunque abbia sottoscritto un qualche servizio online, registrandosi e dovendo fornire alcuni dati personali al gestore del servizio.

Nelle tre slides che seguono riporto estratti da una tipica "informativa sulla privacy", che l'utente incontra quando intende registrarsi ad un servizio offerto via web. L'informativa sul trattamento, richiesta dalla legge, è stata in questo caso frazionata dal titolare del sito web in quattro grandi capitoli (da A a D, nel nostro esempio), a seconda delle diverse finalità del trattamento stesso.

Privacy by Contract
Esempio Consenso

- I dati personali da Lei messi a disposizione del Titolare potranno essere utilizzati:
- (a) (Registrazione) per consentire e gestire la Sua registrazione al Sito;
- (b) (E-commerce) per la gestione ed esecuzione di suoi eventuali ordini di acquisto;

Privacy by Contract / Marketing

(c) Marketing) per l'invio di comunicazioni informative e commerciali, anche di natura promozionale (ivi compresa la nostra newsletter), di materiale pubblicitario e/o di offerte di beni e di servizi, con qualsiasi mezzo (conosciuto o non), ivi compreso, a titolo esemplificativo e non esaustivo, posta, Internet, telefono, E-mail, MMS, SMS dall'Italia o dall'estero (anche da Paesi non appartenenti alla Comunità europea) da parte del Titolare, di società controllanti, controllate e/o partecipate da esso, nonché da parte di entità fisiche o giuridiche legate contrattualmente a Titolare e/o che, comunque, collaborino in attività commerciali del Titolare;

Privacy by Contract / Profilazione

(d) (Profilazione) per consentire la elaborazione ed il compimento di studi e ricerche statistiche e di mercato, nonché per l'analisi dei gusti, delle preferenze, delle abitudini, dei bisogni e delle scelte di consumo da parte del Titolare, di società controllanti, controllate e/o partecipate da esso, nonché da parte di entità fisiche o giuridiche legate contrattualmente al Titolare e/o che, comunque, collaborino in attività commerciali del Titolare.

Come si può vedere, chi deve raccogliere i dati stabilisce anche, ed unilateralmente, la suddivisione delle finalità e delle modalità del trattamento in funzione delle richieste di consenso che deve ottenere da parte dell'utente, consenso che potrebbe essere accordato per alcune finalità e negato per altre. Il tutto avviene in una cornice delineata dalla legislazione e dalla prassi ammessa dal Garante.

Sulla base dell'informativa così predisposta il sito in questione (rectius, il titolare del trattamento) richiede l'autorizzazione (consenso al trattamento dei dati). L'utente può concederla o meno, ma non può negoziare, né su di una più chiara indicazione delle finalità, né su una più analitica suddistinzione delle modalità del trattamento. Non ha modo di incidere per ottenere un ampliamento delle opzioni tra cui scegliere per la prestazione del consenso. Deve aderire o meno allo schema predisposto dal titolare del trattamento.

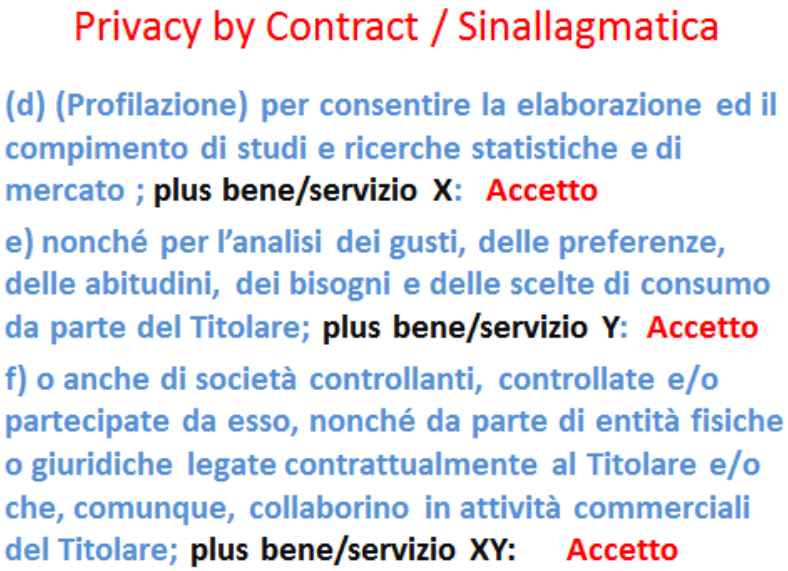
Immaginiamo che fosse invece possibile una negoziazione. Nelle due slides che seguono, nella colonna a sinistra abbiamo il modello stabilito unilateralmente dal titolare del trattamento, in quella di destra un'ipotesi frutto di negoziazione.

Privacy by Contract / Frazionamento

A scelta del solo Titolare	Negoziata
- (a) (Registrazione) per consentire e gestire la Sua registrazione al Sito; - (b) (E-commerce) per la gestione ed esecuzione di suoi eventuali ordini di acquisto. - Accettazione	• (a) (Registrazione) per consentire e gestire la Sua registrazione al Sito; • Accettazione • (b) (E-commerce) per la gestione ed esecuzione di suoi eventuali ordini di acquisto. • Accettazione

Nell'ipotesi negoziata, una prima differenza potrebbe risultare dal maggior frazionamento dei trattamenti da autorizzare, derivante da una richiesta in tal senso da parte dell'utente. L'utente che fornisce i dati, potrebbe così avere più possibilità di scelta. Potrebbe essere per lui preferibile acconsentire solo ad alcune tra le finalità/modalità di trattamento, mantenendo più opzioni rispetto a quelle che il titolare del trattamento tende invece ad offrire quando agisce unilateralmente. La differenziazione sembra offrire vantaggi, non necessariamente solo per l'utente. Un economista saprebbe ben formalizzare questo risultato intuitivo.

In presenza di un'effettiva possibilità di negoziazione, di contrattazione dell'ambito del consenso al trattamento, pur sempre in una cornice stabilita dalla legge, potremmo anche immaginare che chi raccoglie i dati, avendo interesse ad ottenere gli stessi poiché hanno un "valore", sia disposto a fornire qualche forma di incentivo (se non di corrispettivo) per garantirsene il rilascio da parte dell'utente. Provo ad esemplificare nella slide che segue:



Dunque, nell'ipotesi "negoziata" di privacy by contract, le parti segmentano i moduli per la prestazione del consenso. Inoltre, chi raccoglie i dati può offrire incentivi per la prestazione del consenso, crescenti in proporzione della maggiore disponibilità concessa dall'utente in termini di finalità o modalità del trattamento, o anche – si può immaginare - in funzione del crescente numero di dati personali che l'utente fosse pronto a fornire. Gli incentivi potrebbero assumere varia natura. Si immagini l'ipotesi di punti da accumulare per l'ottenimento di sconti per l'acquisto di beni o servizi offerti dal sito.

Nella pratica, in modo implicito, forme di incentivi già esistono (chi si registra ad un sito fornendo l'autorizzazione al trattamento dei dati che fornisce, in genere ottiene servizi aggiuntivi, che spesso peraltro potrebbero essere forniti anche in assenza di registrazione).

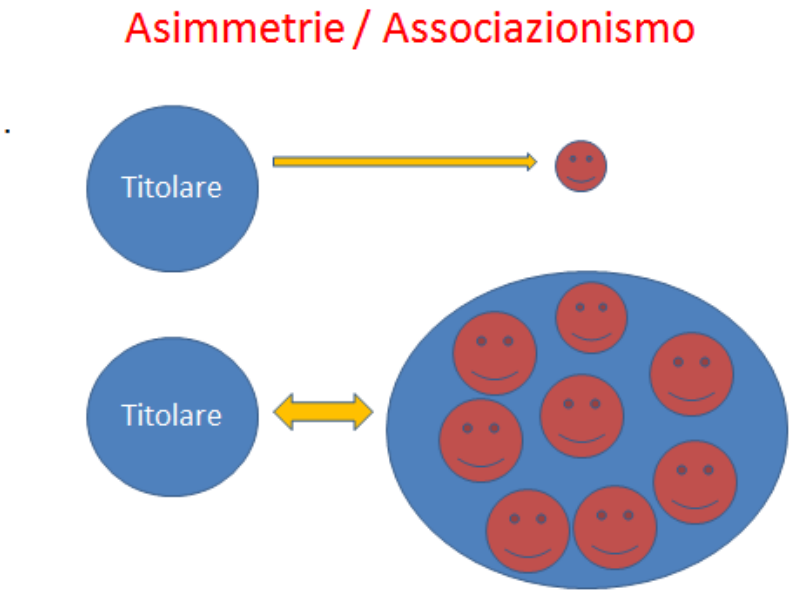
Questo è solo un esempio. La logica sottostante è che se i dati personali costituiscono una valore, ci dovrebbe essere un modo per scambiarlo con trattative e strumenti privatistici, che consentano al creatore dei dati di trattenere una parte del valore che i dati incorporano.

Ovviamente il punto debole di una simile ricostruzione – anche a prescindere dagli ostacoli giuridici - consiste nel fatto che l'utente è un contraente privo di forza negoziale. Considerati gli altri costi di transazione, chi raccoglie i dati (il cosiddetto "titolare" del loro trattamento) non ha interesse, e nemmeno la possibilità, di impegnarsi in una serie indefinita di negoziazioni o

di accordi con i singoli utenti. Inoltre, i dati personali del singolo utente hanno, se considerati isolatamente, un valore quasi irrilevante. Lo schema, in breve, ipotizza una negoziazione senza tenere conto che le parti sono in posizione asimmetrica.

Di qui l'esigenza di ridurre l'asimmetria, di quindi di fornire peso contrattuale al contrente debole e maggior valore ai dati stessi, nonché quella di semplificare gli schemi oggetto di possibile negoziazione, per ridurre i costi di transazione.

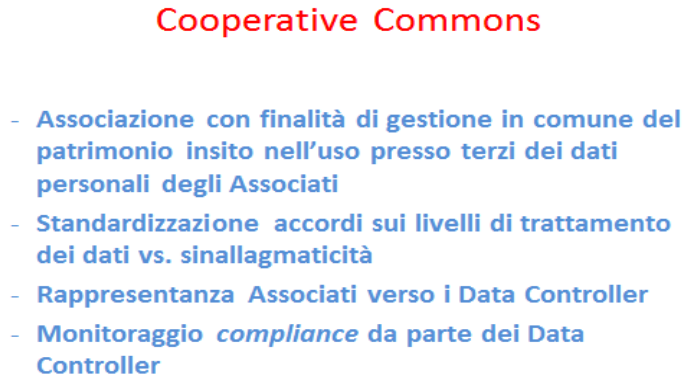
E queste esigenze potrebbero essere soddisfatte attraverso forme di associazione tra gli utenti.



Il gestore del sito web avrebbe così di fronte non il singolo utente, ma un'associazione di utenti. Non il singolo dato personale, ma un insieme significativo di dati. La messa in comune dei dati e dell'interesse alla gestione del loro valore ridurrebbe le asimmetrie e renderebbe meno improbabile l'ipotesi della negoziazione.

Inoltre, l'associazione potrebbe definire moduli standardizzati per la prestazione del consenso, stabilendo clusters predefiniti di finalità e di modalità del trattamento, da fare affermare sul mercato come standard per il rilascio delle autorizzazioni. I diversi moduli potrebbero anche essere graduati in funzione del numero e della qualità dei dati da prestare.

L'associazione, infine, potrebbe occuparsi sia di rappresentare gli associati nella fase di negoziazione, sia di monitorare, sempre per conto della comunità di riferimento, l'interesse al corretto trattamento dei dati ed il rispetto degli accordi raggiunti nell'interesse dei propri associati.



Infine, nell'ottica della privacy by contract, la società cooperativa a scopo mutualistico potrebbe costituire uno strumento collaudato per la rappresentanza di soggetti contrattualmente deboli rispetto alla gestione del servizio in questione sul mercato. I soci della cooperativa partecipano alla società per finalità non direttamente lucrative (cioè intese ad ottenere la remunerazione del capitale di rischio conferito), ma per ottenere altre forme di vantaggio che il mercato non può offrire ai singoli non organizzati. Si tratta di società il cui funzionamento può inoltre rispondere al modello paritario di una testa un voto.

Per questi motivi nel nostro progetto utilizziamo la definizione di "cooperative commons": immaginiamo che la cooperazione organizzata degli utenti, riuniti in società, possa gestire per conto della comunità degli utenti stessi, siano essi soci o meno, un servizio per la gestione dell'autorizzazione all'utilizzo di un bene comune, cioè i dati personali. Gli stessi acquistano valore proprio in quanto aggregati, e gli individui assumono forza e dignità di parte negoziale, realisticamente, solo delegando ad un soggetto che li rappresenti come gruppo organizzato la gestione dei profili patrimoniali inerenti al trattamento dei dati personali. Il movimento cooperativo ha una lunga tradizione nella rappresentanza di istanze consumeristiche e dei soggetti deboli all'interno delle logiche di mercato. Il terreno appare pertanto fertile ed idoneo ad accogliere questa nuova missione.

Questi sono i temi della nostra indagine, ancora agli inizi, ma per la prosecuzione della quale ogni contributo è benvenuto. Nella prossima slide provo a sintetizzare le azioni che mi sembra potrebbero essere intraprese, senza alcuna pretesa di essere esaustivo, ma come traccia di lavoro.

Grazie.

Cooperative Commons – Azioni

- Layer 1: Costituzione società cooperativa a scopo mutualistico (*Joining keen citizens and experts into a cooperative*)
- Layer 2: Sviluppo strumenti tecnologici e giuridici (*Developing tech and legal tools*)
- Layer 3:
- a) Coinvolgimento di studiosi e cittadini nel dibattito culturale (*Engaging scholars and citizens in the debate*)
- b) Rappresentanza cooperatori nei confronti di Big Data (*Agency towards Data controller*)
- c) Pressione verso il legislatore comunitario (*Advocacy with law-makers*)
- d) Monitoraggio rispetto garanzie e accordi sul trattamento dei dati (*Monitoring compliance*)

(Alfonso Papa Malatesta)