Privacy

Alessandro Acquisti*
Carnegie Mellon University

1. - La privacy: Un problema di definizioni

Nel mese di Febbraio del 2002 lo zoo di Washington, DC, negò ad un reporter del *Washington Post* l'accesso ai dati medici e necrologici di Ryma. Rivelare quei dati, spiegò la direttrice dello zoo, avrebbe violato il suo diritto alla *privacy* (Grimaldi, 2002). Quanto più colpisce nella storia di Ryma non è tanto il fatto che la direttrice dello zoo considerasse il suo diritto alla privacy più importante del diritto del pubblico all'informazione, anche dopo la sua morte. Colpisce, invece, il fatto che Ryma era una giraffa. In una nazione in cui è possibile acquistare i dati personali altrui per pochi dollari (inclusi residenza, numeri di telefono, codice fiscale, e via dicendo: Tav. 1), ad un animale morto può venir riconosciuta la protezione di un diritto di cui non sà nemmeno di godere.

Sebbene l'approccio legislativo in materia di *privacy* differisca tra Stati Uniti ed Unione Europea (ed Italia), e sebbene il commercio dei dati personali sia negli USA più aggressivo che nel vecchio continente, la storia di Ryma rivela elementi ricorrenti nel

---

* <*acquisti@andrew.cmu.edu.*>. L'Autore è Assistant Professor of Information Technology and Public Policy presso la H. John Heinz III School of Public Policy and Management, Carnegie Mellon University. L'Autore desidera ringraziare Gustavo Piga per il sostegno in questo lavoro, Giusy Carlevaris per i commenti, ed Eric Chang per alcune ricerche.

[Cod. JEL: D01, D82, D86, G14, L86]

Avvertenza: le traduzioni dall'inglese sono di Antonella Acquisti.

TAV. 1

IL PREZZO DI DATI PERSONALI ACQUISTABILI ONLINE
(legalmente o meno) NEGLI STATI UNITI

Social Security Number (codice fiscale)	10 dollari
Social Security Number, alias, reddito, nome di parenti e vicini	15 dollari
Data di nascita, indirizzo, e numero di telefono	8 dollari
Accesso per un anno a tutti i dati del DMV (motorizzazione civile), inclusi dati su residenza, veicoli di proprietà, violazioni, warrants, etc.	30 dollari
Prezzo medio per una carta di credito rubata su Internet (include nome, numero della carta, data data di scadenza della carta, indirizzo associato alla carta, numero segreto di protezione)	15 dollari

Fonte: varie, ricerca di CHANG E., Carnegie Mellon University.

dibattito sulla *privacy* al di qua e al di là dell'oceano: lo scontro tra interessi contrapposti; le idiosincrasie nell'atteggiamento personale e collettivo verso la *privacy*; e l'ambiguità della sua stessa definizione.

Attraverso i secoli (Westin, 1967) e tra culture diverse per livello di civilizzazione e progresso tecnologico (Murphy, 1964), si ritrova un bisogno comune e ricorrente per la protezione di una sfera privata, un bisogno indefinibile ma imprescindibile di *privacy*. Tale bisogno è riconoscibile sia quando col termine ci si limiti all'attenzione per il trattamento dei dati personali (Agre, 1997), sia quando si intenda un insieme omogeneo (Warren e Brandeis, 1890) o meno (Prosser, 1960) di più ampi diritti personali.

Eppure, non esiste alcuna definizione di *privacy* che ne contenga i molteplici ruoli ed interpretazioni, o che ne metta d'accordo i molti studiosi. Negli anni, la *privacy* è stata interpretata come controllo o come protezione; di un'ampia sfera privata o semplicemente dei propri dati personali; in senso puramente informativo o in senso decisionale. Ed ancora: la *privacy* è stata intesa come solitudine o come intimità, come anonimato o come riservatezza (Westin, 1967). Ed anche quando con *privacy* ci si ri-

ferisca al solo controllo sui propri dati personali, tale controllo è stato riferito alla raccolta, l'uso, o la divulgazione di tali dati.

1.1 *Un diritto o un privilegio?*

Due giovani avvocati di Boston, Samuel Warren e Louis Brandeis, furono tra i primi nel 1890 a definire le coordinate legali della *privacy*. La descrissero sulle pagine della *Harvard Law Review* come il diritto di «essere lasciati (da) soli» (*the right to be left alone*).

La definizione ha incontrato successo, ma in poco più di un secolo di studi la sua portata è stata ripetutamente estesa e ristretta (Tav. 2). Non un concetto organico, ma un termine che collega diritti disparati, per Prosser (1960). Oppure, un aspetto inviolabile della dignità umana, per Bloustein (1964). E ancora: un interesse per la riservatezza dei dati personali, per Turkington (1990). O la libertà di crescere liberi da indebite influenze, per Scoglio (1998). E poi: la *privacy* come abilità di una persona, organizzazione, o governo di controllare il proprio spazio, sia questi una spazio fisico, mentale, o digitale (Sweeney, 2002).

E che valore assegnare alla *privacy*? Alcuni, rifacendosi a Warren e Brandies, la considerano un diritto inalienabile. Altri la vedono come un semplice interesse, da bilanciare con altri (Varian, 1996). Altri ancora considerano la *privacy* un privilegio da non prendere per scontato (Brin, 1998). Altri, un'esigenza indispensabile per il benessere psicologico individuale e l'armonia sociale (Agre e Rotenberg, 1997; Bellotti, 1997; Scoglio, 1998). Ed infine, alcuni vedono nella *privacy* una forma di protezione per l'ipocrisia, l'inganno, e la codardia morale, ed una scusa per il rifiuto delle proprie responsabilità.

Affrontare lo studio della *privacy* significa, dunque, incontrare ambiguità semantiche e contraddizioni. La *privacy* è un valore di per sé positivo per alcuni ma un concetto eticamente neutrale (e dunque conduttivo sia al bene che al male) per altri. La *privacy*, inoltre, può significare qualcosa di diverso persino per la stessa persona in diverse situazioni o momenti della propria vita.

TAV. 2

L'INTERPRETAZIONE DELLA *PRIVACY* CAMBIA NEL TEMPO

Il diritto di essere lasciati da soli	Warren and Brandeis (1890)
Protezione contro indebita pubblicità, appropriazione del proprio nome o immagine, calunnia, intrusioni	Prosser (1960)
Un aspetto della dignità umana	Bloustein (1964)
Controllo sui dati personali	Westin (1967)
Libertà di crescere senza indebite influenze	Scoglio (1998)

Le aspettative su che cosa possa essere considerato privato mutano con fattori come la cultura, l'età, o l'esperienza individuale. Uno stesso individuo potrebbe accettare di buon grado l'idea che l'azienda del telefono registri i numeri di telefono che egli chiama; ma potrebbe non accettare che il suo fornitore di collegamento Internet possa monitorare i siti che egli frequenta.

Il concetto di *privacy*, inoltre, cambia nel tempo con il progredire di costumi sociali, cultura, e tecnologia, perché con essi cambiano anche i confini tra pubblico e privato.

Per un viaggiatore europeo del XVIII secolo, condividere un letto in una locanda con un altro viaggiatore sconosciuto sarebbe stata cosa assai inusuale. Eppure tale pratica era comune nello stesso periodo nell'America dei coloni (Smith, 2000).

Gli stessi Warren e Brandeis nel 1890 reagivano all'uso intrusivo di una nuova tecnologia: la fotografia istantanea, che, insieme all'evoluzione commerciale dei quotidiani di costume, aveva reso pubblici aspetti un tempo privati della vita dell'*intelligenzia* bostoniana di fine secolo.

Oggi le nostre aspettative sul ruolo e l'uso di tecnologie di ripresa e monitorizzazione in pubblico sono diverse: siamo quasi indifferenti alla presenza di macchine fotografiche per le strade o telecamere a circuito chiuso nei negozi. Alcuni accettano di avere telecamere televisive dentro le proprie case, e decidono di vi-

vere la propria vita constantemente sotto gli occhi di un pubblico anonimo.

Eppure, gli sviluppi tecnologici continuano a cambiare le carte in gioco: microscopiche macchine fotografiche e video camere inserite dentro telefoni cellulari possono dare seconda giovinezza alla protesta di Warren e Brandeis (1890), stimolando la richiesta di risposte normative in Italia (Muti, 2004) e altrove.

La *privacy*, dunque, è un concetto dalle molteplici, mutabili, ed a volte contraddittorie interpretazioni, che rimandano alla continua dinamica di negoziazione tra pubblico e privato. È possibile che tra dibattiti semantici, idiosincrasie, mutamenti culturali, e contraddizioni, la scienza economica possa contribuire alla comprensione del soggetto? È utile discutere gli aspetti economici della *privacy*? E cosa significa l'economia della *privacy*?

2. - Le radici economiche della *privacy*

Ben prima che la *privacy* generasse interesse tra gli economisti, argomentazioni etiche o morali in favore o meno della sua protezione nascondevano ragioni economiche, se non esplicitamente monetarie (Acquisti, in stampa).

In epoche diverse, per esempio, censimenti governativi incontrarono resistenze popolari non soltanto dovute alla naturale diffidenza verso le intrusioni dell'autorità, ma anche a motivazioni economiche: i censimenti sono stati spesso usati dai governi per determinare l'entità delle tassazioni da imporre alle popolazioni. Nel caso americano, Smith (2000) racconta che nel 1799 gli agenti del governo federale statunitense furono mandati a registrare il numero e la dimensione delle finestre delle case di privati cittadini per stabilire le loro imposte. Ci fu quasi una rivolta: «[i]l cuore della protesta era senza dubbio la resistenza alle tasse, anche se la retorica della protesta si concentrò sul rifiuto all'intrusione nella vita privata». (Smith, 2000, p. 40).

Anche la protezione di dati demografici può nascondere motivazioni economiche dietro le giustificazioni morali. Intorno alla metà del 1600, ad esempio, «[l]e autorità della [Colonia della Baia

TAV. 3

UN ESEMPIO DI *TRADE-OFFS* DELLA *PRIVACY*: CONSUMATORE E VENDITORE *ONLINE*

		Benefici	Rischi
I dati del consumatore non vengono rivelati durante la transazione	Per il consumatore	Non c'è discriminazione sul prezzo, c'è un senso di protezione/sicurezza	Non ci sono servizi personalizzati o sconti in cambio di dati personali, ci sono costi dovuti alla protezione dei dati
	Per il venditore	Reputazione positiva	Meno dati sui consumatori da usare per vendita o *marketing*
I dati del consumatore vengono rivelati durante la transazione	Per il consumatore	Ci sono servizi personalizzati o sconti in cambio di dati personali	C'è discriminazione sul prezzo, c'è il rischio di incorrere in costi futuri dovuti alla rivelazione di dati personali
	Per il venditore	Abilità di discriminare attraverso il prezzo, abilità di servire il consumatore in maniera migliore	Timori dei consumatori per la *privacy* possono peggiorare l'interazione con il venditore

Fonte: ACQUISTI A. (2002*b*).

del] Massachusetts [decisero di] proteggere i dati [demografici raccolti tra la popolazione dei coloni.] Si rifiutarono di rivelare dati sui tassi di mortalità [nella colonia,] non tanto per proteggere l'identità dei coloni, ma nel timore che quelle informazioni, una volta note, potessero rendere la colonia meno attraente ai potenziali futuri coloni inglesi» (Smith, 2000, pp. 12-13).

E ancora: mentre la reazione di Warren e Brandeis all'uso di fotografie istantanee nei giornali del tempo non aveva un connotato chiaramente economico, il successo commerciale di quei giornali, dovuto anche a tali nuove intrusioni nella *privacy* altrui, certamente lo aveva.

Durante il ventesimo secolo, con la riduzione dei costi di registrazione, manipolazione, ed uso di dati personali (in particolare in forma digitale), lo scontro tra interessi economici contrapposti è diventato trasparente.

Su Internet, per esempio, l'informazione che un visitatore rivela ad un sito può essere usata per rendere la navigazione più piacevole o efficiente, ma anche per anticipare a scopo di lucro il comportamento del consumatore e la sua propensione all'acquisto di certi prodotti. Questo comporta sia benefici che possibili costi per il visitatore ma anche per il gestore del sito (Tav. 3).

Famoso è diventato per le ripercussioni negative il tentativo di *Amazon.com* nel 2001 (un sito Internet che vende libri, CD musicali, ed altri prodotti), di usare l'informazione personale dei suoi clienti per differenziarne il prezzo di offerta, ovvero, per fornire lo stesso prodotto a prezzi diversi a diversi individui. La pratica, presto scoperta, causò ad *Amazon.com* danni di immagine e di reputazione che spinsero la società a rimborsare ai consumatori i plusvalori guadagnati (Streifield, 2001; Acquisti e Varian, 2005).

2.1 Privacy *e* trade-offs

Rifacendoci a Westin (1967) e Noam (1996), possiamo interpretare lo scontro tra gli interessi contrapposti nelle questioni di *privacy* come un processo di negoziazione tra le opposte esigenze della sfera privata e della sfera pubblica. In questo processo emergono *trade-offs* non soltanto tra le varie parti (il soggetto e coloro con i quali il soggetto può interagire), ma anche, individualmente, per ciascuna parte coinvolta (Tav. 4).

Da un lato, individui, imprese, o governi vogliono conoscere quanto più possibile delle persone con cui hanno a che fare (amici, clienti, cittadini che pagano le tasse, e via dicendo), facendo però attenzione ad evitare gli effetti controproducenti del superare i limiti dell'altrui tolleranza all'invasione della propria sfera privata. Dall'altro, gli individui hanno interesse a rivelare ad altri informazioni personali (per ottenere migliori servizi o trattamenti, o per soddisfare un naturale bisogno di apertura, comunica-

TAV. 4

TRADE-OFFS E DUALITÀ STILIZZATE DELLA *PRIVACY*

Privacy	Scambio di dati personali
Vantaggi ottenuti e costi evitati quando i dati personali sono protetti	Vantaggi ottenuti e costi evitati quando i dati personali sono scambiati
Costi incorsi e vantaggi persi quando i dati personali sono protetti	Costi incorsi e vantaggi persi quando i dati personali sono scambiati

Fonte: ACQUISTI A. (2002*b*).

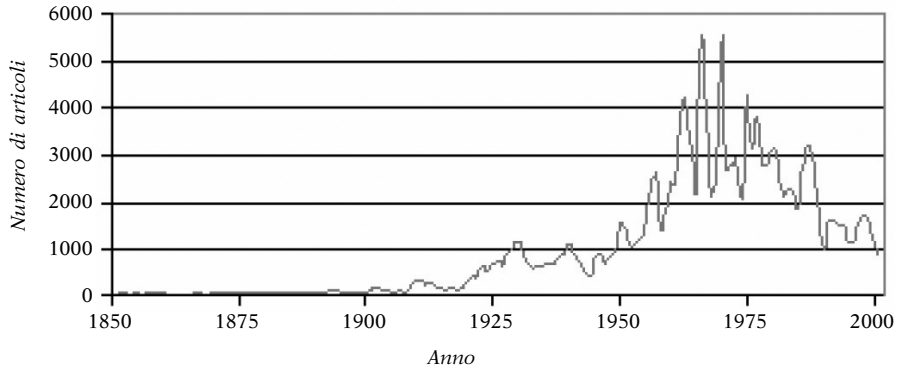
zione, ed interazione), ma non vogliono che tali informazioni vengano sfruttate abusivamente o siano usate a loro danno.

Questi *trade-offs* assumono rilevanza economica crescente con lo sviluppo delle tecnologie dell'informazione, che a partire dagli anni sessanta diventano sempre più comuni nella vita di burocrazie, imprese, e cittadini. La *privacy* diventa di moda (Graf. 1), in particolare nell'accezione di protezione di dati personali (Westin, 1967). Ma studiare il bilanciamento di *trade-offs* ed interessi in competizione tra loro è l'oggetto della scienza economica. Dunque, alla fine degli anni settanta, nasce l'economia della *privacy*, come lo studio delle conseguenze economiche della protezione (o meno) di dati personali.

Studiare i *trade-offs* della *privacy* in un'ottica economica, tuttavia, non significa credere che la protezione della *privacy* sia sempre riconducibile a considerazioni finanziarie: anche se le scelte individuali e della società in merito all'uso di informazioni private hanno spesso implicazioni pratiche, molte delle conseguenze della protezione o diffusione di dati personali non sono quantificabili in termini monetari. Dunque l'economia della *privacy* studia i *trade-offs* e gli incentivi reali e potenziali che emergono nella dinamica di interazione tra sfera privata e sfera pubblica, ma studia anche quali condizioni di quei *trade-offs* massimizzino il benessere sociale ed individuale, e come quelle condi-

GRAF. 1

NUMERO DI ARTICOLI PUBBLICATI DAL NEW YORK TIMES CONTENENTI LA PAROLA *PRIVACY* 1850-2001



Fonte: CHITRA KALYANARAMAN, Carnegie Mellon University.

zioni possano essere raggiunte dal mercato: tramite intervento legislativo? attraverso autoregolamentazione? grazie alla responsabilità individuale nell'uso di tecnologie di invasione e di protezione dei dati?

Poiché in questi *trade-offs* economici tecnologia e legge sono inestricabilmente legate, per capire l'economia della *privacy* è necessario prima discutere delle tecnologie che la invadono e di quelle che la proteggono, così come delle iniziative normative che la regolano nei diversi paesi.

3. - Invasioni e reazioni

3.1 *Le tecnologie di invasione*

Progressi tecnologici, in particolare nell'area dei sistemi di informazione, trasformano la dinamica e la concezione di pubblico e privato, creando nuove opportunità di interazione tra individui e nuovi rischi per la *privacy* (Tav. 5).

TAV. 5

I NUMERI DELL'INVASIONE DELLA *PRIVACY*

Numero di telefoni sotto sorveglianza negli Stati Uniti nel 1997	237.000
Numero di conversazioni telefoniche sotto sorveglianza negli Stati Uniti nel 1997	Due milioni e mezzo
Stima del costo di furti e frodi di identità nel 2002 negli Stati Uniti	1,4 miliardi di dollari
Costo medio subito da vittime di furti di identità negli Stati Uniti	18.000 dollari (minimo: 250 dollari; massimo: oltre 200.000 dollari)
Numero di telecamere di sorveglianza in Gran Bretagna	Oltre 1 milione e mezzo
Numero medio di volte che, in una giornata, una persona a Londra viene ripresa da una telecamera di sorveglianza	300 volte
Numero di vittime di *phishing* (frodi via *email*) nel 2003	1 milione, con circa 1,2 miliardi di danni
Percentuale di traffico *Internet* di *emails* classificabile come *spam* nel 2004	62%
Stima del numero di *email* classificabili come *spam* spedite nel 2003 nel mondo	4.900 miliardi
Stima del tempo medio perso per ogni messaggio di spam (scaricando il messaggio, aprendolo, cancellandolo, etc.)	3 secondi
Prezzo del servizio base di anonimato di navigazione *Internet* offerto da *Anonymizer.com*	Gratis
Prezzo del servizio completo di anonimato di navigazione *Internet* offerto da *Anonymizer.com*	Circa 90 dollari

Fonte: Varie.

Il telegrafo nel 1844 ed il telefono nel 1876 allargarono le frontiere della comunicazione umana, ma resero anche possibili nuove forme di sorveglianza nella vita altrui. L'operatore necessario a completare le chiamate dai primi telefoni era libero di rimanere in linea ed ascoltare le telefonate in corso. Le stesse linee telefo-

niche (così come quelle del telegrafo) erano condivise tra i pochi utenti, rendendo possibile monitorare le conversazioni altrui.

Anche dopo la sostituzione degli operatori con deviatori automatici rimase possibile per governi (e quant'altri interessati), mettere il naso nelle comunicazioni di altre persone con tecnologie di sorveglianza. Nel 1997, nei soli Stati Uniti, il governo registrò circa due milioni e mezzo di conversazioni.

Nel 1887, Herman Hollerith innovò il processo di manipolazione dei dati con le sue «schede perforate», mettendo in moto un processo che avrebbe condotto allo sviluppo dei computer (Hollerith fondò la società che poi divenne IBM), ma anche allo sviluppo commerciale delle banche dati di informazioni pesonali.

Nel 1888, la Kodak rese facile ed economico immortalare le immagini della propria vita famigliare (Smith, 2000), ma anche quelle della vita altrui, provocando la reazione di Warren e Brandeis.

Nel ventesimo secolo, progressi in campo biometrico (dallo studio delle impronte digitali alle analisi del DNA), di registrazione video e audio, e di miniaturizzazione hanno ripetutamente influenzato le aspettative individuali di *privacy*. La diffusione di tecnologie digitali (ed in particolare, la diffusione dei personal computers e di Internet) ha agito come catalizzatore per altre tecnologie in termini di protezione o violazione della *privacy*. Negli ultimi anni, la riduzione del costo di memorizzazione delle informazioni ha permesso a governi ed imprese di catturare, conservare, ed analizzare quantità crescenti di dati su ogni individuo. Il costo di un *gigabyte* di memoria su disco rigido era quasi 12.000 dollari nel 1988, 13 dollari nel 2001 e meno di un dollaro nel 2003 (Acquisti e Varian, 2005). Le aziende oggi possono registrare digitalmente i dettagli di ogni transazione con i loro clienti, ogni sito Internet può studiare in dettaglio il comportamento *online* dei suoi visitatori, molti governi possono collegare tra loro dati personali da fonti differenti per creare dossier individuali, ma anche privati cittadini possono creare banche dati personali sul comportamento proprio ed altrui. Più le organizzazioni ed i consumatori adottano tecnologie digitali, e meno costosa e più veloce diventa la produzione e lo studio dei dati personali.

Molte attività giornaliere ormai sono o possono essere monitorizzate elettronicamente, e lasciano una scia elettronica del soggetto che il soggetto stesso non può controllare. Froomkin (2000) e Garfinkel (2000) evidenziano alcune delle tecnologie che possono essere usate per sorveglianza, e alcuni dei modi in cui è possibile ricostruire la vita quotidiana di una persona: transazioni ai bancomat, con carte di credito, o bollette; telecamere con tecnologie di riconoscimento visivo automatico usate in spazi pubblici (come aeroporti e stadi); banche dati per impronte digitali e DNA; tecnologie senza fili e satellitari usate per sorveglianza geografica — da GPS (*Global Positioning System*) a RFID (*Radio Frequency Identification*) — in telefoni, automobili, banconote, o anche prodotti come frigoriferi o vestiti; applicazioni che registrano l'esatta sequenza di battute ad una tastiera di un computer di un'impresa o di un ignaro utente; spyware che studia il comportamento dell'utente di un computer e ne trasmette i dati personali a terzi; intercettazione e monitorizzazione (manuale o automatica) di messaggi di posta elettronica, *instant messaging*, o navigazione Internet; sistemi di sorveglianza globale di trasmissioni digitali come Echelon (White, 2002); *cookies* per identificare, riconoscere, e monitorare i visitatori di un sito; numeri di identificazione nascosti in prodotti elettronici hardware e software — dai chip nei computer ad applicazioni grafiche o stampanti — che rivelano dati ad altri sistemi senza la conoscenza o l'autorizzazione del possessore di quei prodotti; e via dicendo. Froomkin (2000) conclude che «l'effetto di insieme e cumulativo di queste tecnologie può rendere la vita moderna completamente visibile e trasparente» a osservatori a noi sconosciuti: «non c'è nessun posto in cui ci si possa nascondere» (Froomkin, 2000, p. 1461).

Tutte queste informazioni possono entrare in banche dati, il più delle volte separate e distinte. Ma quelle banche dati possono anche essere confrontate, collegate, e combinate per ricostruire attraverso tecniche di *data mining* stime accurate, profili dettagliati, o dossier completi del comportamento e delle attività di ogni persona. Questo spesso accade non solo senza consenso ma anche senza che l'interessato ne sia a conoscenza.

3.2 *Conseguenze*

Mentre il problema della *privacy* non è nuovo (né lo è il mercato per le informazioni personali), nuova è l'abilità di raccogliere, manipolare, studiare, e reagire ad una massa di dati personali in tempo reale senza intervento umano. È diventato non soltanto tecnologicamente possibile ma economicamente efficiente creare sistemi informativi che sostituiscono agenti umani nell'inferenza e deduzione basata su dati individuali.

Che la monitorizzazione, la trasmissione, e l'uso di dati personali senza controllo dei diretti interessati siano in aumento è cosa non controversa. Controversa, invece, è la valutazione delle conseguenze di tali transazioni, quando i loro costi (in termini di invasioni della *privacy*) vengano confrontati ai vantaggi in termini di efficienza, qualità di prodotti, o velocità di servizio che quelle stesse transazioni rendono possibili.

Anche se sono stati avanzati approcci ispirati all'analisi dei costi e benefici (Stewart, 1996), valutare gli effetti complessivi delle transazioni di dati personali non è facile. Le conseguenze positive o negative del rispetto della *privacy* o della sua violazione sono spesso stime incerte nel tempo, potenziali, ed intangibili, mentre i pesi da assegnare nel confronto dei vari fattori sono inevitabilmente soggettivi per individui ed organizzazioni.

3.2.1 Gli individui

Per gli individui, non soltanto il desiderio di *privacy* si scontra con bisogni opposti, come quello di comunicare, vivere in comunità con altri, esibirsi, o condividere; ma la *privacy* può anche offrire copertura all'ipocrisia e all'inganno, o alla fuga dalle proprie responsabilità (Schoeman, 1984).

I vantaggi della *privacy* nella sua accezione più ampia sono dunque spesso intangibili. Possono risiedere nel benessere psicologico di una persona che la *privacy* protegge, nella libertà di esprimersi e di comportarsi senza censura sociale, nella protezione dallo stigma sociale (Regan, 1995; Scoglio, 1998; Lessing,

1999). Altri benefici sono più tangibili, seppure non necessariamente in chiave monetaria: la protezione contro forze o influenze ostili o contro gli errori di terzi, o l'abilità di mantenere confidenziali certe informazioni essenziali per il proprio successo.

Definizioni più circoscritte della *privacy* mostrano *trade-offs* nei mercati duali della *privacy* e dei dati personali più facilmente quantificabili, e spesso monetari.

Da un lato, ci sono molteplici costi di invasione, come lo *spam* via email, la pubblicità postale spazzatura, o il *telemarketing* via telefono. Ci sono anche i costi in termini di discriminazione del prezzo o offerte selettive dovute al *profiling* del consumatore (Zettelmeyer *et* al., 2001). L'individuo può a volte proteggersi, ma ad un costo: rifiutandosi di fornire certi dati (e forse vedendosi negato il servizio), offrendo dati falsi (e perdendo i vantaggi della personalizzazione), o proteggendo i dati tramite varie tecnologie (Sezione 3.3.2) (ed incorrendo nei molteplici costi di apprendimento e di utilizzo).

Dall'altro lato, l'individuo può anche trarre benefici tangibili ed immediati dalla rivelazione di informazioni personali: compensazioni monetarie (come sconti, premi, partecipazione a lotterie) in cambio di dati personali; servizi personalizzati, trattamenti preferenziali, e via dicendo.

Tuttavia, anche costi in principio quantificabili sono spesso incerti, protratti nel tempo, o potenziali. Per descrivere tale situazione Varian (1996) usa la metafora dell'"assegno in bianco", che l'individuo firma quando rivela informazioni personali ad altre parti. L'informazione rivelata durante una transazione potrebbe in seguito essere usata per servire meglio il consumatore, ma anche per danneggiarlo: se, come, quando, e con quali conseguenze ciò avverrà non è dato sapere. Discriminazioni, errori involontari nell'uso dei dati, o l'uso di dossier per vendetta, ricatto, o semplice influenza sono eventualità difficili da definire e prevedere. In sostanza, l'individuo è raramente in grado di giudicare i rischi che derivano dalla rivelazione dei propri dati a parti terze, come burocrazie, imprese, o altri individui (Swire e Litan, 1998).

3.2.2 Le organizzazioni

Aziende, burocrazie, o semplici individui possono trarre grande vantaggio dalla conoscenza di informazioni personali di clienti, cittadini, e conoscenti. Un'impresa, ad esempio, può migliorare le strategie di *marketing* mirando a specifici segmenti di mercato (Blattberg e Deighton, 1991), o implementare varie forme di discriminazione del prezzo. Le aziende o i governi locali possono anche ricavare dalla vendita di dati di clienti ed utenti ad altre organizzazioni.

L'ente che guadagna dall'uso o dalla rivendita di quei dati non soffre dei costi che il soggetto dei dati potrebbe subire (Swire e Litan, 1998). L'esistenza di un mercato secondario dei dati personali crea dunque esternalità economiche per il consumatore: le aziende internalizzano i benefici ma non assorbono i costi di uso dei dati personali altrui.

Per le imprese, i costi per monitorare, conservare, analizzare, manipolare e trasmettere dati personali continuano a diminuire, mentre l'abilità di collegare dati da fonti diverse per inferire conclusioni tramite *data mining* continua ad aumentare.

Tuttavia, anche l'abilità di creare e mantenere sofisticate banche dati non è senza costo. Vi sono costi di sviluppo, costi derivanti da errori nei dati (e il tentativo di eliminarli), costi di tecnologie di protezione dei dati stessi (sviluppate per rispondere alle domande del mercato o della legge), ed i costi legali, economici, o di reputazione dovuti alle intrusioni perpetuate dalle stesse imprese (Gellman, 2002). Inoltre, nel timore di invasioni della *privacy*, alcuni consumatori non concludono transazioni, non offrono dati personali, o li offrono sbagliati: secondo *Jupiter Research* (2002), ad esempio, venditori *online* perdono miliardi di dollari ogni anno in vendite mancate per via dei timori dei clienti per la propria *privacy*.

Nel passato poche aziende hanno valutato questi costi tali da giustificare politiche di gestione dei dati meno intrusive. L'equilibrio economico risultante però potrebbe non essere efficiente.

Da un lato, la qualità dell'informazione nelle mani delle aziende può giovare al bene comune: non soltanto le aziende possono

ridurre i costi di contatto dei clienti (non importunando i consumatori non interessati ma non dimenticando quelli interessati) e riducendo i prezzi di offerta; ma diventa anche possibile offrire prodotti di nicchia (altrimenti troppo rischiosi da produrre in assenza di dettagliate informazioni di mercato: Blattberg e Deighton, 1991) o fornire prodotti più vicini alle preferenze individuali.

Dall'altro lato, i costi sociali di errori ed incompletezze in banche dati commerciali, mediche, o governative possono diminuire in presenza di un mercato dei dati personali ben consolidato (Laudon, 1996).

Una combinazione appropriata di protezione e condivisione di dati personali potrebbe dunque soddisfare gli interessi delle varie parti, riducendo costi ed invasioni ma aumentando i vantaggi e l'accuratezza. Resta da vedere se la legge, la tecnologia, o il mercato siano in grado di realizzare quella combinazione.

3.3 *Le reazioni*

3.3.1 La legge

Di fronte al rapido progresso delle tecnologie dell'informazione ed i nuovi equilibri di potere che esse determinano tra soggetti e possessori di dati, molte nazioni si sono rivolte alla legge per regolare lo scambio di informazioni personali.

L'approccio del legislatore americano in materia di *privacy* è assai diverso da quello del legislatore italiano e quello europeo. Di fronte alla complessità del problema, il legislatore americano ha scelto una strada utilitarista, ispirata al libero mercato delle idee e basato su autoregolamentazione e *standards* calibrati per aree specifiche, come il settore bancario, medico, o l'affitto di videocassette (Reidenberg, 1995). L'approccio del legislatore americano è dunque settoriale (l'equilibrio tra protezione e scambio di dati è valutato di settore in settore), decentralizzato (le leggi vigenti sono molte e disparate), e incline alla deregolamentazione e al *laissez faire*.

L'approccio del legislatore europeo (e del legislatore italiano) è invece ispirato a principi etici di giusto trattamento dei dati personali: è un approccio generalista (assume un diritto alla *privacy* independente dal settore di applicazione), centralizzato (tale diritto è prottetto attraverso un codice unico), e normativo. Questo approccio ha influenzato la Direttiva europea sulla protezione degli individui per quanto riguarda il trattamento dei dati personali (European Parliament, 1995), accolta in Italia con l'entrata in vigore, il primo Gennaio del 2004, del «Codice della *privacy*».

I due modelli (europeo/italiano e statunitense) hanno però l'identico scopo di proteggere la *privacy* dell'individuo senza colpire i bisogni di flussi informativi di ogni economia avanzata.

I vantaggi del sistema americano sono la sua efficienza e adattabilità. Economisti di scuola neoclassica preferiscono questo approccio, basato sulle iniziative del mercato fino al punto di "propertizzare" l'informazione privata e creare un mercato nazionale dei dati personali (Varian, 1996; Laudon, 1996; Varian e Shapiro, 1997). I suoi rischi, però, sono la moltiplicazione dei codici e delle interpretazioni e la protezione dello *status quo*, che a volte lascia il cittadino indifeso contro violazioni della sua *privacy ex-ante* o senza mezzi per compensare errori e violazioni *ex-post*. Bellotti (1997) scrive: «questa incertezza determina lunghe cause legali per determinare se e quale violazione di *privacy* sia occorsa» (p. 67).

Considerati i limiti dell'approccio deregolamentato, altri studiosi hanno proposto alternative legali, come la negoziazione di licenze per l'uso dei dati personali e la protezione di quei dati al pari di segreto commerciale (Samuelson, 2000), o la protezione della *privacy* tramite responsabilità civile (*tort law*) (Litmann, 2000).

Tuttavia, visto che l'individuo è spesso in una posizione di svantaggio nei confronti delle organizzazioni con cui interagisce, l'argomento economico può anche essere usato per favorire un approccio legislativo che superi i limiti di difese puramente contrattuali (Samuelson, 2000), o per suggerire risposte tecnologiche ai problemi di *privacy*.

3.3.2 La tecnologia

Il progresso delle tecnologie dell'informazione non crea soltanto nuovi rischi di invasione della *privacy*, ma offre agli individui anche nuovi strumenti per rispondere a quelle invasioni (Agre e Rotenberg, 1997; Clarke, 1999).

L'abilità del consumatore di negoziare con altre parti il livello desiderato di condivisione di dati personali è cresciuta in anni recenti grazie a progressi tecnologici.

Una di queste tecnologie è la crittografia (Froomkin, 1995; Goodlatte, 1998), il processo di creare e decifrare comunicazioni segrete. Dati personali "crittati" sono trasformati in codici non interpretabili senza una chiave segreta. L'informazione personale crittata è dunque protetta sia che viaggi su Internet, che risieda nel *computer* del soggetto, o che sia conservata in una banca dati commerciale.

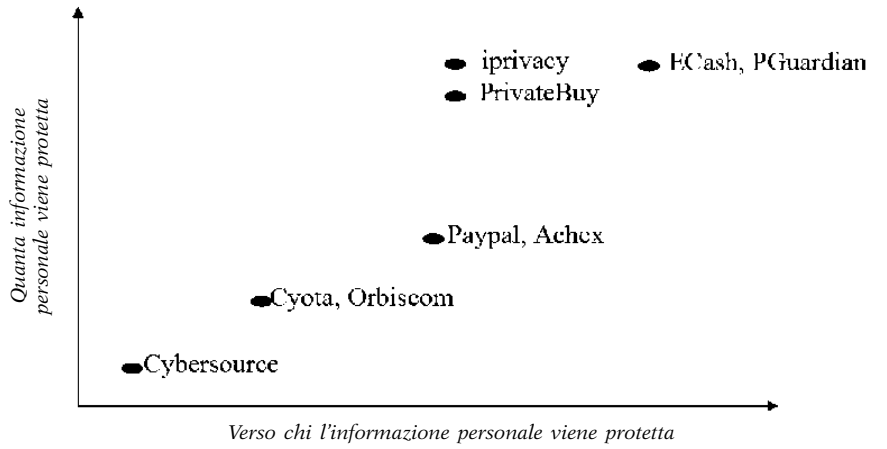
Il mero atto di crittare dati personali, però, non risolve ogni problema di *privacy*. In primo luogo, l'utilizzo di dati crittati non può essere unilaterale: un individuo non può mandare ad un venditore dati personali prottetti tramite crittografia a meno che il venditore non li accetti in tale forma. In secondo luogo, una volta decifrati da parti terze autorizzate, i dati non sono più protetti e sfuggono nuovamente al controllo del soggetto. In terzo luogo, la crittazione dei dati personali non protegge la *privacy* di individui le cui attività possono essere desunte da altre fonti.

Tuttavia, dagli anni ottanta in poi, le procedure di crittazione sono state usate in un numero crescente di protocolli che non mascherano semplicemente i dati, ma aiutano a salvaguardare la *privacy* di un individuo in diverse transazioni.

Grazie a certi protocolli è possibile concludere transazioni confidenziali con parti terze sconosciute (Jones *et* al., 1995; Winsborough *et* al., 2000; Camp, 2000); completare pagamenti elettronici senza rivelare dati finanziari (Chaum, 1983, Graf. 2); mandare messaggi elettronici non riconducibili al mittente (Chaum, 1981); navigare su Internet senza rivelare ad altre parti i siti visitati o il computer usato per la navigazione (Goldschlag *et* al., 1999; Reiter e Rubin, 1999); votare elettronicamente garantendo la cor-

GRAF. 2

IL MERCATO PER LE TECNOLOGIE DI PAGAMENTO ELETTRONICO, ANONIME E NON ANONIME NEL 2001



Fonte: Autore.

rettezza dei risultati senza compromettere la segretezza del voto (Benaloh e Yung, 1986; Benaloh, 1987); condividere dati, preferenze, ed interessi con altri senza rivelare la propria identità (Adar e Huberman, 2001; Canny, 2002); creare sistemi di credenziali anonime (Chaum, 1985; Chaum e Evertse, 1985; Camenisch e Lysyanskaya, 2001); e via dicendo.

Alcuni di questi protocolli separano i dati personalmente identificabili da quelli non riconducibili all'individuo (Ware, 1985). Altri dividono l'informazione confidenziale tra vari gruppi di agenti (Bellotti, 1997). Altri ancora mirano a proteggere la *privacy* tramite l'anonimato, nascondendo i dati e le azioni di un individuo con quelle di molti altri (Acquisti *et* al., 2003) o con un traffico di dati artificiali generati per mantenere l'anonimato di un individuo in una folla di altri individui.

L'anonimato è una forma di *privacy* dell'identità (Goldberg, 2000). È lo stato di essere sconosciuti o non riconoscibili in un gruppo (Diaz *et* al., 2002; Serjantov e Danezis, 2002). Esso richiede il controllo o l'eliminazione di ogni collegamento tra dati che po-

trebbero collegare una certa azione (per esempio, mandare una lettera minatoria) alla persona che l'ha compiuta (il mittente della lettera). Un avversario con sufficienti risorse o incentivi, però, potrà quasi sempre trovare elementi sufficienti a ricostruire l'identità di una persona. Ma non è ancora possibile usare questi attacchi su scala globale (Lundblad, 2004). Dunque è sufficiente rendere gli attacchi miranti a risalire all'identità di una persona non impossibili ma semplicemente troppo costosi. La questione tecnologica diventa allora una questione economica: le tecnologie di anonimato proteggono la *privacy* rendendo la missione di un avversario troppo costosa per essere completata.

Mascherare o nascondere i dati di un individuo non sono le sole forme di protezione tecnologica della *privacy*. Jiang *et* al. (2002) distinguono fra tecnologie che puntano sulla prevenzione di invasioni della *privacy* (impedendo la monitorizzazione, l'uso, o la disseminazione di dati personali — la crittografia e le tecnologie di anonimato fanno parte in genere di questo gruppo); quelle che mirano a minimizzare o annullarne le conseguenze (per esempio, informando gli individui dei rischi correnti); e quelle che mirano a rilevare eventuali violazioni ed invasioni.

Molte di queste tecnologie di protezione (*privacy enhancing technologies*, o "PET") sono già a disposizione del mercato grazie agli sforzi di società private e centri di ricerca (Brunk, 2002; Tav. 2). Con esse è diventato più facile proteggere dati confidenziali senza interrompere la divulgazione di informazioni necessarie al completamento di una transazione. Meno facile si è rivelato convincere il mercato ad adottare queste tecnologie.

3.3.3 Gli individui e il mercato

Dagli studi di Alan Westin (Westin, 1967, 1991) in poi (Spiekermann *et* al., 2001), ricerche empiriche sulla *privacy* hanno individuato tre categorie di persone: quelli che si mostrano pragmaticamente pronti a rivelare dati personali quando convenga; i "fondamentalisti", che dicono di voler protegger i propri dati e credono in un diritto alla *privacy* e nel dovere degli altri di

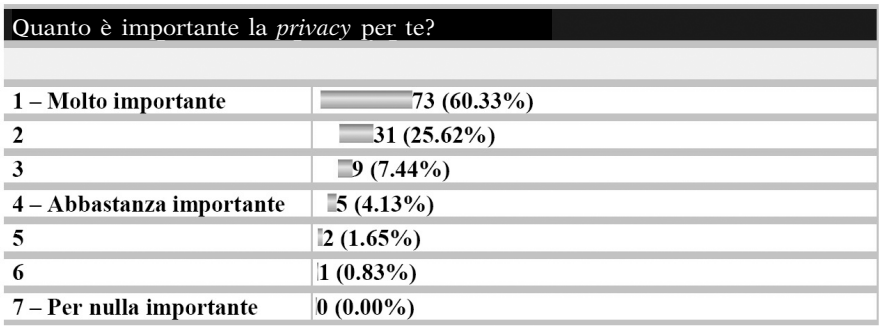
rispettare quel diritto; e i "rilassati", che sembrano non nutrire particolari preoccupazioni per la *privacy* dei propri dati.

Pragmatici e fondamentalisti sono le tipologie più comuni. Negli Stati Uniti, interviste e studi mostrano che la preoccupazione del cittadino medio per la propria *privacy* è elevata. Nel 2000 uno studio della *Federal Trade Commission* trovò che il sessantasette per cento dei consumatori americani erano "molto preoccupati" riguardo alla tutela della *privacy* dei dati personali forniti *online* (Federal Trade Commission, 2000). In uno studio condotto alla Carnegie Mellon University nel 2004 sono stati trovati risultati simili (Acquisti e Grossklags, 2005, Graf. 3). In tale studio, i soggetti si sono dichiarati particolarmente preoccupati per il rischio che dati personali di tipo diverso vengano collegati tra loro senza il consenso del soggetto (per esempio, qualora il nome e cognome riportati su una carta di credito vengano collegati al profilo *online* ed ai dati di navigazione registrati sui cosiddetti *cookies,* Tav. 6).

Questi timori causano danni alle stesse organizzazioni (Sezione 3.2.2). Secondo uno studio di *PriceWaterhouseCoopers*, nel 2000 i consumatori americani avrebbero fatto più acquisti *online*

GRAF. 3

ATTITUDINI VERSO L'IMPORTANZA DELLA *PRIVACY*.
CAMPIONE DI 119 INDIVIDUI
ALLA CARNEGIE MELLON UNIVERSITY



Fonte: ACQUISTI A. - GROSSKLAGS J. (2005).

se i siti commerciali avessero meglio protetto i dati personali (ebusinessforum.com, 2000). Secondo *Jupiter Research* «entro il 2006 si perderanno 24,5 miliardi di dollari a fronte dei 5,5 miliardi del 2001. Le vendite al dettaglio online potrebbero essere incrementate di circa il ventiquattro percento nel 2006 se le paure del consumatore riguardo *privacy* e sicurezza fossero indirizzate efficacemente» (Jupiter Research, 2002).

Eppure, poche delle tecnologie di protezione hanno trovato successo nel mercato o hanno registrato livelli di adozione significativi (Bruilk, 2002). Studi (Jupiter Research, 2002) ed esperimenti (Spiekerman *et* al., 2001) hanno infatti mostrato che anche gli individui che si dichiarano più preoccupati per la loro *privacy* sono pronti a rivelare dati personali in cambio di piccoli sconti e vantaggi limitati.

Questa dicotomia tra attitudine e comportamento è stata osservata in svariati aspetti della psicologia umana e studiata nella letteratura psicologica nel sociale fin dai tempi di LaPiere (1934) e Corey (1937). Molte possono essere le ragioni per cui compare

TAV. 6

LIVELLI DI PREOCCUPAZIONE PER LA DIFFUSIONE DI DATI PERSONALI. CAMPIONE DI 119 INDIVIDUI ALLA CARNEGIE MELLON UNIVERSITY

	Dati personali	Profilo Online	Dati professionali	Identità sessuale e politica	Dati personali e profilo online combinati insieme
Preoccupazione Elevata	38,3%	25,0%	11,7%	11,7%	58,3%
Preoccupazione Media	46,7%	40,8%	50,0%	25,0%	29,2%
Preoccupazione Bassa	11,7%	33,3%	36,7%	60,0%	10,8%
Dati mancanti	3,3%	0,8%	1,7%	3,3%	1,7%

Fonte: ACQUISTI A. - GROSSKLAGS J. (2005).

nelle questioni di *privacy*: i costi e le difficoltà di utilizzo delle tecnologie di protezione (Whitten e Tygar, 1999); gli *switching costs* collegati al cambiamento nel proprio comportamento in termini di uso di dati personali; l'ignoranza dei rischi derivanti dalla divulgazione di dati personali; la tendenza verso la gratificazione immediata (Acquisti, 2004*b*); o ancora, l'impossibilità di proteggersi contro ogni possibile invasione o rischio per la *privacy* (Tav. 7); o infine, la difficoltà stessa delle aziende tecnologiche nel fornire soluzioni di protezione della *privacy* che soddisfino gli interessi ed i bisogni delle varie parti.

TAV. 7

CHI USA LE TECNOLOGIE DELLA PRIVACY?
CAMPIONE DI 119 INDIVIDUI
ALLA CARNEGIE MELLON UNIVERSITY

Il 74% del campione ha adottato almeno una strategia tra le seguenti:

– Usare crittografia per proteggere le proprie *email*
– Inserire il proprio numero di telefono in liste che i *telemarketers* non possono chiamare
– Interrompere una transazione qualora manchino i presupposti di protezione dei dati
– Rivelare dati falsi
– *Altra strategia*

Tuttavia, solo l'8% usa crittografia per le proprie email, il 9% distrugge documenti contenenti dati personali prima di buttarli, ecc.

Fonte: ACQUISTI A. - GROSSKLAGS J. (2005).

4. - L'economia della *privacy*

4.1 Privacy *e dati personali come beni economici*

La reazione degli individui e del mercato ai problemi di *privacy* è complessa. A volte confidiamo segreti solo ad una cerchia ristretta di conoscenti; altre volte riveliamo dettagli personali a sconosciuti che non avremo più occasione di incontrare. Da un lato, il bisogno di *privacy* è diffuso nella società; dall'altro gli stru-

menti tecnologici offerti per proteggerla vengono ignorati, e piccoli incentivi sono sufficienti a convincerci a rivelare informazioni personali.

Alla radice di queste complessità risiede la duplice asimmetria informativa (Akerlof, 1970) dei problemi di *privacy*. La prima forma di asimmetria informativa riguarda la *privacy* intesa come controllo sull'informazione personale: implica che il soggetto conosce cose di sé che ad altri non è dato sapere. La seconda forma di asimmetria informativa nasce quando il soggetto ha perso il controllo dei propri dati, e non può più sapere come, quando, da chi, o per quali ragioni saranno usati. In un'era di tecnologie dell'informazione onnipresenti ed invisibili il soggetto spesso non si accorge nemmeno quando questa seconda forma di asimmetria informativa entri in gioco.

Entrambe le forme di asimmetria informativa determinano esternalità (Sezione 3.2.2) e problemi di azzardo morale: i costi di una bancarotta sono subiti dal creditore che non conosceva i dettagli preoccupanti del passato del debitore; ma i costi di una intrusione nella banca dati di un venditore (che espone i numeri di carta di credito del cliente alla mercé dell'*hacker*) sono, in assenza di protezione legale, subiti dal cliente stesso. Il venditore ha anzi pochi incentivi ad investire nella sicurezza dei dati del consumatore

Nelle economie moderne, la seconda forma di asimmetria informativa sembra influenzare pesantemente la bilancia del potere tra individui ed organizzazioni. Per il soggetto dei dati dunque diventa assai difficile valutare sia il valore dei propri dati che il valore della propria *privacy*. Questi valori sono spesso deducibili solo *ex-post* (ovvero quando i dati vengano usati in un certo modo o la *privacy* venga invasa), ed in combinazione con altri dati (per esempio, la somma dei rischi dovuti alla divulgazione separata di una *password* e di un acconto che usa quella *password* è inferiore al rischio congiunto di rivelare i due dati insieme). È difficile inoltre separare i costi oggettivi delle violazioni della *privacy* (come i danni economici dovuti al furto di identità) dalla sensibilità soggettiva verso i problemi di *privacy* indipendentemente da quei costi.

Dunque le decisioni che riguardano la *privacy* richiedono difficili considerazioni in due aree collegate ma distinte: da un lato il mercato dei dati personali, dall'altro il mercato della *privacy* (intesa come controllo di quei dati). Il primo è il mercato delle società di intermediazione informativa, come i *data marketers* e le agenzie di credito. Il secondo è il mercato della protezione dei dati, come le applicazioni tecnologiche. Ciascun mercato ha caratteristiche e dinamiche specifiche. Il problema della *privacy* è così interessante dal punto di vista economico perché tocca entrambi i mercati allo stesso tempo.

4.2 *L'evoluzione dell'economia della* privacy

I primi articoli sul mercati dei dati ed il mercato della *privacy* di taglio esplicitamente economico appaiono nella letteratura verso la fine degli anni settanta. Il dibattito è vivace ma dura dopo pochi anni. L'interesse non ritorna che alla metà degli anni novanta, sotto l'influenza di nuove tecnologie di invasione e protezione di informazione digitale. Dopo il 2000, il numero di articoli (inclusi quelli contenenti modelli formali) cresce rapidamente.

4.2.1 A cavallo tra gli anni settanta e gli anni ottanta

Dopo la seconda guerra mondiale l'economia dell'informazione diventa una delle aree di ricerca più importanti degli studi economici. Rifacendosi a Friedrich Hayek (economista di scuola austriaca), alcuni studiosi iniziano ad interpretare tutta la teoria economica come economia dell'informazione, a partire dal valore principalmente informativo che il "prezzo" assume in un'economia di mercato.

Hirshleifer, nel 1971, aveva già discusso l'uso privato dell'informazione, la sua protezione, e la sua divulgazione, ma riferendosi all'informazione tecnologica, non personale. Espliciti studi economici sulla *privacy* dell'informazione personale appaiono

nella letteratura economica e legale soltanto alla fine degli anni settanta, con i contributi di Posner (1978, 1981); Hirshleifer (1981); Stigler (1981), ed altri collaboratori al numero di Primavera 1978 della *Georgia Law Review* e il numero di Dicembre 1980 del *Journal of Legal Studies*.

Sono economisti e giuristi della cosiddetta scuola di Chicago (come Posner e Stigler) ad animare il dibattito con tesi utilitariste e posizioni liberiste.

Posner (1978) interpreta la *privacy* puramente come il "nascondere" (*concealing*) informazione — un diritto che si scontra con un altro diritto rilevante sia per l'economista che per il giurista: il diritto di altri a "sapere". Posner ritiene che un corollario della protezione della *privacy* intesa come controllo del flusso di informazioni che riguardano una persona, sia la possibilità che questi si presenti ad altri in maniera non veritiera. Questa abilità crea un conflitto con l'interesse altrui ad avere informazioni accurate sul conto di una persona con cui si stiano instaurando dei rapporti. La *privacy* personale dunque può risultare dannosa per la società.

Al contrario, sono le imprese, scrive Posner, che dovrebbero ricevere una maggiore protezione legale al fine di mantenere segrete informazioni cruciali per la loro competitività. Mettendo a confronto la persona fisica e la persona giuridica, Posner conclude che negli Stati Uniti la tendenza verso interventi legislativi che impongono obblighi di trasparenza alle imprese ma maggiore *privacy* per gli individui sia un esempio di «perversa regolazione del governo della vita economica e sociale» (p. 26).

Tale posizione, comune tra gli autori della Scuola di Chicago, è chiaramente antagonista verso interventi regolatori, considerati non soltanto non necessari, ma probabilmente dannosi. È questa una visione lontana dalla sensibilità europea in materia di *privacy*. Sebbene incontri l'opposizione di filosofi ed altri giuristi o economisti (come Hirshleifer), questa è la voce dominante del pensiero economico del tempo.

Stigler (1980), per esempio, ritiene che non sia necessario interferire in transazioni volontarie tra agenti economici per proteggere una delle parti (purché le condizioni "usuali di competi-

zione" siano presenti). In assenza di interventi normativi, in una libera transazione di dati individuali sarà rivelato un ammontare equo ed efficiente di informazione personale, in base ai desideri di *privacy* e conoscenza delle diverse parti. Per esempio, ogni individuo ha interesse a rivelare dati personali quando da questi risulti una immagine positiva (per esempio, nel contesto della richiesta di un prestito, una persona è interessata a rendere nota la propria reputazione di buon debitore). Per contro, un individuo è interessato a celare informazioni negative (per esempio, qualora sia consapevole di non godere di un buon credito). Ma così facendo, l'individuo che cela i suoi dati si rivela agli altri come un individuo con caratteristiche indesiderabili, il che porta la controparte ad alzare i prezzi dei servizi (in questo caso, il prezzo del credito). Stigler conclude che l'assenza di leggi che vietino al creditore di passare informazioni sul debitore ad altri finisce per proteggere il debitore stesso.

Al contrario, la protezione della *privacy*, secondo Stigler, peggiora la qualità dei dati sugli agenti economici (come il livello di produttività di un prestatore d'opera). L'impatto è dunque economicamente inefficiente e ridistributivo. È inefficiente, perché le risorse (come quelle umane) saranno usate in maniera poco efficace qualora manchino informazioni accurate sulla loro qualità; ma anche perché la ridotta abilità di riconoscere la qualità individuale diminuisce anche l'abilità di ricompensarne in modo equo le differenze (ciò, a sua volta, indurrà i possessori di certe risorse a investire di meno nel migliorarne la qualità). Il risultato è anche ridistributivo, perché se la difficoltà di misurare le differenze tra gli individui aumenta, il loro trattamento (ad esempio salariale) diventa più omogeneo, con conseguente ridistribuzione di reddito dai lavoratori qualitativamente migliori a quelli con le qualità peggiori.

Un'analisi simile si trova in Posner (1981): negare ad altri informazioni su di noi è causa di inefficienze, trasferisce il costo di eventuali carenze dell'individuo da questi ad un altro soggetto (per esempio, il datore di lavoro), e ritarda il processo in cui imprese e lavoratori si incontrano su livelli di efficienza. Questo ritardo, a sua volta, può finire per colpire negativamente anche il mercato dei lavoratori più produttivi.

Posner (1981), rifacendosi a Prosser (1960), ammette che certe forme di protezione della *privacy* basate sulla responsabilità civile (*tort law*) abbiano valide basi economiche: per esempio, la protezione contro l'appropriazione dell'altrui nome o immagine; contro la diffusione di informazioni calunniose o tendenziose; o contro metodi intrusivi di accesso all'informazione personale, come lo spionaggio e la sorveglianza. E già Hirshleifer (1980), nel 1980, avrebbe criticato le posizioni di Posner e Stigler, notando che gli studi economici delle interazioni di mercato basate su agenti economici freddamente razionali e puramente egoistici posono essere validi strumenti di ricerca, ma tali modelli di comportamento umano non rappresentano adeguatamente le interazioni che avvengono fuori dalla logica di mercato, come nel caso della *privacy*.

Con l'eccezione di queste poche critiche, però, la posizione del pensiero economico dominante a cavallo tra gli anni settanta e ottanta è sostanzialmente *anti-privacy*.

4.2.2 Gli anni novanta

L'eco delle critiche di Hirshleifer (1980) torna a influenzare il pensiero economico dopo circa 15 anni di scarso interesse per l'economia della *privacy*. Solo intorno alla metà degli anni novanta il progresso delle tecnologie digitali dell'informazione (con la moltiplicazione di banche dati elettroniche e *personal computers*, lo sviluppo delle tecnologie di crittografia, la nascita di Internet, la diffusione della posta elettronica, ed il moltiplicarsi degli usi secondari di dati personali) attraggono di nuovo l'attenzione degli economisti.

Varian (1996) nota come lo sviluppo di tecnologie a basso costo per la manipolazione dell'informazione abbia creato nuove preoccupazioni per il trattamento dei dati personali. Tuttavia, Varian ritiene che vietare ogni trasmissione di dati personali non sia nell'interesse dell'individuo stesso. Un consumatore ha interesse a rivelare certe informazioni (come i suoi gusti in materia di prodotti, così da ricevere notizie sui prodotti che hanno richiamato

la sua attenzione, evitando quelle su prodotti non graditi) e tenerne altre nascoste (quanto sia disposto a pagare per un certo bene). I problemi nascono, dunque, quando troppa poca informazione utile viene scambiata.

Questo ragionamento ha qualcosa in comune con gli approcci di Stigler e Posner. Tuttavia, Varian nota pure che l'uso secondario dei dati personali costituisce una esternalità economica. Anche se due parti trovano un accordo per il trasferimento di dati personali dall'una all'altra, quest'ultima potrebbe poi fornire questi dati a terzi per usi diversi da quelli che le due parti avevano inizialmente concordato. Questo uso secondario dei dati potrebbe creare costi per l'individuo a cui l'informazione si riferisce.

Anche Noam (1996) riprende ma aggiorna gli argomenti della scuola di Chicago, rifacendosi agli studi di Coase. Secondo il cosiddetto teorema di Coase, in assenza di costi di transazione, l'assegnamento iniziale di diritti di proprietà è arbitrario ed ininfluente in termini di efficienza del mercato e dell'equilibrio che vi si determina. Nel caso della *privacy*, per esempio, Noam sostiene che tra una parte con un certo interesse a proteggere la propria informazione ed una controparte interessata ad ottenerla, prevarrà semplicemente la parte per cui è maggiore l'interesse, indipendentemente dalla protezione inizialmente accordata dal sistema legale. Per questa ragione, l'uso della crittografia e di tecnologie per la protezione dei dati personali non determinano tanto il risultato finale della transazione (quale parte finisca per avere controllo dei dati personali), ma lo scambio di valore da una parte all'altra nel processo. Poiché i consumatori a partire dalla metà degli anni novanta hanno accesso a nuove tecnologie per la protezione della loro *privacy*, le controparti che vogliano ottenere i loro dati devono offrire in cambio di dati una valida compensazione. Dunque la crittografia, conclude Noam, finirà per trasferire ricchezza al consumatore.

Questa combinazione di analisi tecnologica ed economica si trova anche in Laudon (1996), che propone un "mercato nazionale dell'informazione" in cui agli individui venga riconosciuta la proprietà dei loro dati e l'abilità di alienarla ad altri dietro compenso. Come gli economisti della scuola di Chicago, Laudon cre-

de che la protezione puramente legale della *privacy* sia datata. Come Varian, Laudon crede che un sistema basato su diritti di proprietà dell'informazione personale possa servire agli interessi dei consumatori ma anche delle imprese. Di qui la sua proposta di soluzione mista di mercato, tecnologia, e regolazione.

4.2.3 La nuova economia della *privacy*

Le tecnologie dell'informazione che alla metà degli anni novanta avevano riacceso l'interesse per gli aspetti economici della *privacy* diventano con *Internet* fenomeni di massa. Il numero sempre maggiore di individui con accesso a tecnologie che lasciano indelebili tracce elettroniche porta la *privacy* al centro del dibattito politico e culturale (Graf. 4). Sull'onda di questi cambiamenti, a partire dal 2000 prende slancio un nuovo filone di ricerca sull'economia della *privacy*.

Alcune caratteristiche distinguono questo nuovo filone dagli studi precedenti. Gli studi sono adesso formali, basati su veri e

GRAF. 4

LA *PRIVACY* SULLE
PRIME PAGINE DI RIVISTE AMERICANE NEL 2000

proprio modelli matematici (spesso microeconomici) che analizzano l'equilibrio del mercato della *privacy*. Inoltre, l'oggetto di studio non è ristretto all'informazione personale (anche se lo studio della *privacy* come confidenzialità dei dati personali rimane il cuore della ricerca): mentre Posner nel 1981 escluse dallo studio economico la *privacy* come «pace e quiete» e la *privacy* come «libertà ed autonomia», appaiono adesso studi sui costi, per l'individuo, di intrusioni nella quiete personale, come la posta commerciale indesiderata (o *spam*: Png *et* al., 2003) o delle preferenze personali verso la *privacy* (Tang *et* al., 2004). Inoltre, in alcuni modelli, viene considerata la possibilità che i consumatori non agiscano come agenti economici puramente razionali (Taylor, 2004*a*; Acquisti, 2004*b*; Acquisti e Varian, 2005), un'ipotesi, quella di razionalità, cara alle teorie della scuola di Chicago. Infine, mentre l'approccio della scuola di Chicago era basato su una visione piuttosto unidimensionale della *privacy*, la ricerca economica più moderna nota la complessità del concetto di identità ed accoglie definizione più sfumate su che cosa siano i dati personali. Per esempio, Acquisti (2002*a*) distingue identità *online* ed *offline* di una stessa persona ed evidenzia come certi dati personali possano essere trasferiti dal soggetto ad altri agenti con beneficio di entrambi (ed incremento del *welfare*), mentre altri dati possono rimanere protetti, di nuovo con beneficio dei vari agenti. La *privacy* dunque non è vista solo come una variabile dicotoma, ma come un continuo dalle molte dimensioni.

Acquisti e Varian (2005) studiano l'interazione di consumatori e imprese in un mercato in cui le imprese possono usare tecnologie per identificare e riconoscere i consumatori da una transazione all'altra, ed i consumatori hanno a disposizione tecnologie per evitare di essere identificati e riconosciuti. Mostrano che le tecnologie per l'individuazione dei consumatori (per esempio, i *cookies* di un sito Internet) non garantiscono necessariamente all'impresa un incremento dei profitti, a meno che l'impresa non usi quelle stesse tecnologie anche per fornire servizi addizionali e personalizzati ai consumatori.

Taylor (2004*a*) studia un problema simile, il mercato per i dati personali dei consumatori. Per un'impresa, il valore dei dati per-

sonali del consumatore deriva dall'abilità di riconoscere il consumatore e offrirgli prezzi "personalizzati", prezzi che l'impresa prevede che il consumatore non rifiuterà (una forma di discriminazione del prezzo). In presenza di tecnologie che permettono queste strategie, il benessere economico collettivo dipende dall'abilità dei consumatori di prevedere come saranno usati i loro dati personali. Se i consumatori non si rendono conto che le loro decisioni possono rivelare ad un gruppo di imprese la loro disponibilità a pagare per un certo bene, il *surplus* di una transazione finirà soltanto nelle tasche delle aziende (a meno che un regime legale imponga la protezione della *privacy* e vieti lo scambio di dati sui consumatori tra diverse imprese). Se i consumatori invece anticipano l'uso dei loro dati da parte delle imprese, il regime normativo non è necessario: diventa interesse delle imprese stesse proteggere i dati dei loro consumatori anche in assenza di regolamentazione. La ragione, come in Acquisti e Varian (2005), sta nel fatto che consumatori razionali possono rendere controproducenti le strategie di invasione della *privacy* da parte dell'impresa.

Calzolari e Pavan (2001) considerano un problema simile: lo scambio di dati dei consumatori tra due imprese. Le imprese sono interessate a sapere quanto un certo consumatore sia disposto a pagare per un certo bene. Calzolari e Pavan mostrano che la trasmissione di informazioni personali dei consumatori da un'impresa ad un'altra può ridurre le distorsioni informative inerenti al mercato e dunque migliorare il benessere generale: rivelare informazioni non necessariamente diminuisce il profitto del consumatore, infatti, potrebbe contribuire ad un miglioramento delle condizioni per tutte le parti. Inoltre, Calzolari e Pavan mostrano che sotto certe condizioni il venditore potrebbe decidere di proteggere l'informazione del consumatore anche senza intervento normativo.

Sembrerebbe che questi risultati supportino le ragioni della scuola di Chicago: il mercato tenderà a generare la distribuzione efficiente dei dati personali anche senza interventi regolatori come la Direttiva europea o il Codice della *privacy* italiano. Tale conclusione sarebbe affrettata.

In primo luogo, diversi studi a partire dal 2000 mostrano che al di fuori di scenari stilizzati le forze del mercato spesso non so-

no sufficienti a determinare i risultati economicamente più efficienti. Taylor (2004*b*) dimostra che anche in presenza di consumatori razionali le imprese hanno un incentivo ad investire più risorse del livello socialmente ottimale nel raccogliere dati personali. Png *et* al. (2003) mostrano come in un mercato competitivo con diverse tipologie di consumatori (quelli che non traggono nessun valore dalla posta commerciale non richiesta, e quelli che sono interessati a ricevere informazioni su nuovi prodotti) i tentativi dei consumatori di usare tecnologie per evitare *marketing* indesiderato e gli sforzi dei venditori di usare *marketing* diretto sono "complementi strategici", nel senso che l'aumento dell'uno finisce, perversamente, per far aumentare anche l'altro.

Inoltre, sia Acquisti e Varian (2005) che Taylor (2004*a*) mostrano come, in presenza di consumatori non perfettamente razionali, le regole del mercato possano non risultare sufficienti a garantire la protezione della *privacy*. Acquisti (2004*b*) mette in evidenza le difficoltà che l'individuo deve affrontare nel prendere decisioni sulla propria *privacy* (questo argomento è discusso di seguito).

Infine, i modelli formali qui sopra esaminati studiano l'individuo come un astratto agente economico. L'informazione personale che viene studiata in questi modelli è, nella maggior parte dei casi, semplicemente la valutazione personale di un certo bene (e dunque la somma di denaro che il consumatore sarebbe pronto a pagare, e che il venditore ha interesse a conoscere per aumentare il proprio *surplus* dalla transazione). Al di fuori dei modelli teorici, però, ma dentro le economie reali, le transazioni tra consumatori e imprese non rivelano soltanto la disposizione di un individuo verso un certo bene, ma molta altra informazione: per esempio, il nome del consumatore, il numero della sua carta di credito, il suo indirizzo postale, e via dicendo. Questi dati addizionali possono causare addizionali costi alla *privacy*: dai furti di identità alle truffe via carta di credito. Non appena si inizi a distinguere tra pseudonimi ed identità (Friedman e Resnick, 2001; Acquisti, 2004*a*) emergono problemi di *privacy* che vanno al di là dei ragionamenti e risultati della scuola di Chicago e dei modelli teorici basati su astratti agenti economici. Emergono anche,

tuttavia, opportunità per soddisfare le esigenze delle varie parti proteggendo certi dati condividendone altri con beneficio reciproco (Acquisti, 2002*a*).

4.3 *Il dibattito attuale*

Tra le molte direzioni che la ricerca sull'economia della *privacy* ha intrapreso dal 2000 ad oggi, due sono particolarmente interessanti: la valutazione dei costi della *privacy*, e la relazione tra *privacy*, incentivi economici, e comportamento individuale.

4.3.1 I costi della *privacy*

Si è già discussa (Sezione 3.2) la distinzione tra due tipi di costi della *privacy*: i costi subiti da una o l'altra parte quando la *privacy* di una parte venga violata; ed i costi cui si va incontro nel proteggere la *privacy*

I costi di intrusione colpiscono sia gli individui che le stesse imprese. Per il consumatore, possono includere i costi fisici o psicologici dovuti all'intrusione in uno spazio privato (dalla casella email nel caso di posta elettronica indesiderata, alla violazione dell'intimità della propria casa con fotografie scattate via teleobbiettivo, o altro); la perdita di opportunità commercialmente favorevoli per via di paure legate alla *privacy*; la diminuzione del valore della propria informazione personale, che viene diluita dall'uso fattone da altri; la maggiore esposizione a truffe e costi futuri (come il furto di identità o le truffe via carta di credito); nonché le perdite di tempo ed i costi non misurabili. Per le imprese, i costi possono provenire da spese legali dovute alle loro invasioni nella *privacy* altrui o alla negligenza nel proteggere l'altrui informazione. I costi possono anche provenire dall'erosione della qualità di interazione con il consumatore, qualora questi perda fiducia nell'impresa (in casi estremi, il consumatore può decidere di abbandonare un'impresa che non offre sufficienti garanzie di protezione della *privacy*). Gellman (2002) quantifica i costi di intru-

sione nell'ambito dell'economia americana nell'ordine di decine di miliardi di dollari all'anno.

Dal lato opposto, alcuni economisti puntano l'attenzione sui costi dovuti alla protezione della *privacy*, ovvero i costi che gli individui devono sostenere per usare tecnologie di protezione della *privacy*, ma anche i costi che le imprese o le agenzie governative devono affrontare per decisione propria o per adeguarsi ad eventuali normative (Rubin e Lenard, 2002). Staten e Cate (2003) trovano che i costi causati da regolamentazioni che richiedono *opt-in* (cioè esplicito assenso dell'individuo all'uso dei suoi dati) nel mercato del credito sono ingenti. Tra questi costi sono inclusi anche quelli subiti da imprese e individui qualora non venisse scambiata informazione sufficiente: in assenza di informazione adeguata, sia l'individuo che l'impresa potrebbero andare incontro ad errori costosi. Inoltre, i costi di opportunità potrebbero risultare significativi: per esempio, la perdita di opportunità preziose per entrambe le parti quando, per proteggerne la *privacy*, il consumatore non venga informato sull'uscita di un nuovo prodotto di probabile gradimento.

Quali tra queste tipologie di costi (di intrusione e di protezione) siano più significative è oggetto di acceso dibattito tra chi crede nella *privacy* prima di tutto come un diritto (e dunque tende a favorire iniziative normative che aumentino gli incentivi per la sua protezione); e chi, concentrandosi sulle sue implicazioni, preferisce il libero scambio di informazione gestito dal mercato e dall'individuo.

4.3.2 Incentivi individuali e comportamento[1]

L'individuo incontra spesso difficoltà a valutare opportunamente costi e incentivi in materia di *privacy*. Esperimenti (Spiekermann *et* al., 2001) ed interviste hanno mostrato che anche i consumatori più sensibili alle questioni di *privacy* sono in genere disposti a fornire dati personali in cambio di sconti an-

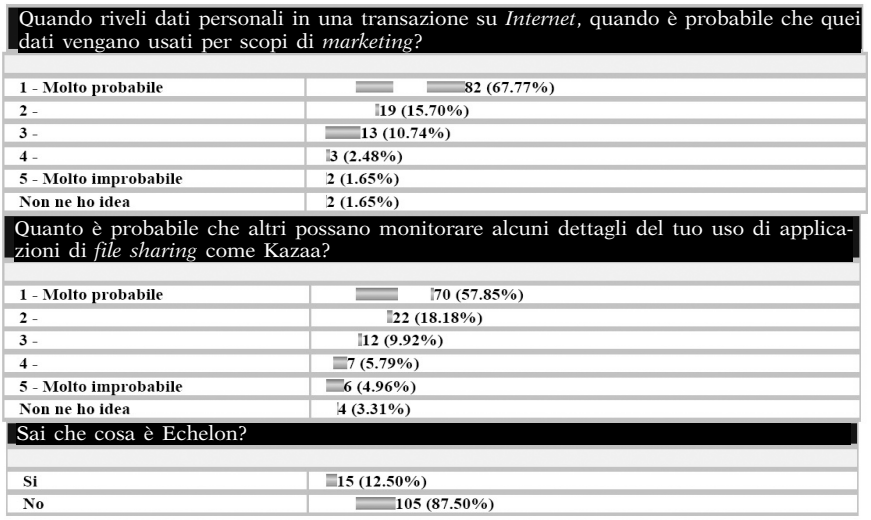
[1] Parti di questa sezione sono basate su ACQUISTI A. (2004*b*).

che poco significativi. In genere, i consumatori hanno mostrato scarso interesse per l'uso delle tecnologie di protezione offerte sul mercato. Acquisti e Grossklags (2004), Acquisti (2004*b*), ed Acquisti e Grossklags (2005) hanno esaminato queste apparenti contraddizioni nel processo di decisione individuale per quanto riguarda la *privacy*. Questo processo è ostacolato da una serie di fattori, tra cui *incomplete information* (informazione incompleta), *bounded rationality* (razionalità limitata), e una serie di deviazioni sistematiche dalla strategia ottimale di un agente puramente razionale discusse nella letteratura dell'economia del comportamento (Kahneman e Tversky, 2000).

Informazione incompleta. A quali informazioni l'individuo ha accesso quando si prepara a prendere decisioni sulla *privacy* dei propri dati? Per esempio, è consapevole delle possibili violazioni conseguenti una certa transazione, e dei rischi ad esse associati? È a conoscenza delle tecnologie che proteggono tali dati? (Graf. 5.)

GRAF. 5

CONSAPEVOLEZZA ED IGNORANZA DI RISCHI PER LA *PRIVACY*.
CAMPIONE DI 119 INDIVIDUI
ALLA CARNEGIE MELLON UNIVERSITY



Fonte: ACQUISTI A. - GROSSKLAGS J. (2005).

Come sopra notato, le transazioni economiche sono spesso caratterizzate da informazione incompleta o asimmetrica. Informazioni incomplete influiscono in vari modi sul processo decisionale sulla *privacy*.

È difficile per un individuo valutare questi valori, soprattutto quando le transazioni di dati personali e le violazioni della *privacy* diventano onnipresenti ed invisibili.

Molte conseguenze associate alla protezione della *privacy*, o alla sua violazione, possono essere scoperte o accertate solo a posteriori. Si consideri, per esempio, le difficoltà nell'usare le tecnologie legate alla *privacy* e alla crittografia descritte in Whitten e Tygar (1999). In aggiunta, i calcoli impliciti nei *trade-offs* della *privacy* dipendono da informazioni incomplete riguardo la probabile distribuzione di eventi futuri. Alcune di queste distribuzioni possono essere previste dopo aver messo a confronto dati; per esempio, la probabilità che da una certa transazione con carta di credito risulti una frode può essere calcolata usando dati già esistenti. La distribuzione delle probabilità di altri eventi può essere stimata senza garanzia di accuratezza a causa della enorme dinamicità del mercato dei dati personali; per esempio, è verosimile calcolare la probabilità che certi dati, rivelati adesso, saranno usati fra cinque anni per un furto d'identità? E la distribuzione di probabilità di molti altri eventi può essere quasi totalmente soggettiva: si consideri la probabilità che una nuova forma di attacco ad un sistema di crittazione attualmente sicuro possa, fra qualche anno, svelare tutte le nostre comunicazioni personali adesso opportunamente protette. Ciò ci porta ad un secondo problema: quello della razionalità limitata.

Razionalità limitata. Siamo capaci di calcolare tutti i parametri importanti per le nostre scelte in materia di *privacy*? O siamo condizionati dai limiti della nostra razionalità? Nel nostro contesto, la razionalità limitata si riferisce all'incapacità di calcolare e confrontare le dimensioni dei benefici associati alle varie strategie che l'individuo può scegliere nelle decisioni che riguardano la *privacy*. La razionalità limitata si riferisce anche all'incapacità di vagliare tutte le informazioni stocastiche correlate ai rischi e alle probabilità di eventi legati ai costi e ai benefici. Nella teoria

economica tradizionale, all'agente si attribuisce sia la razionalità che un potere computazionale senza limiti di vagliare le informazioni. Ma gli esseri umani non sono in grado di vagliare tutte le informazioni in loro possesso e trarre da esse conclusioni accurate (Simon, 1982). Nello scenario che consideriamo, l'individuo, dopo aver fornito ad altre parti in causa informazioni personali, perde letteralmente il controllo sulle stesse per intervalli di tempo imprevedibili. L'individuo che rivela ad altri dati (senza nemmeno il suo consenso o la sua conoscenza) assume una posizione di asimmetria informativa per quel che riguarda l'uso e la disseminazione degli stessi dati da parte di altri. Dunque, i costi cognitivi collegati al tentativo di calcolare una strategia ottimale in materia di *privacy* possono essere così alti che l'individuo spesso ricorre a semplici euristiche.

Deviazioni sistematiche. Infine, anche se l'individuo avesse accesso ad informazioni complete e potesse appropriatamente usarle con tempo e capacità illimitate per raggiungere una decisione in ogni questione rilevante per la *privacy*, potrebbe ancora trovare difficoltà nel seguire una strategia ottimale.

Un vasto corpo di letteratura in economia e psicologia ha ormai confermato l'impatto di svariate forme di "alterazioni" comportamentali e psicologiche sul processo di decisione individuale. La *privacy* sembra essere un caso-studio che comprende molte di queste alterazioni: sconto iperbolico, sotto assicurazione, problemi di autocontrollo, gratificazione immediata, ed altri.

Gli individui hanno, per esempio, una tendenza a scontare in maniera "iperbolica" costi o benefici futuri (Rabin e O'Donoghue, 2000; O'Donoghue e Rabin, 2001). In economia lo sconto iperbolico implica un'inconsistenza di preferenze personali nel tempo; eventi futuri possono essere scontati a tassi di sconto differenti rispetto ad eventi più prossimi. Lo sconto iperbolico può influenzare decisioni sulla *privacy*, per esempio quando si scontino pesantemente la (bassa) probabilità di un (alto) rischio futuro quale il furto d'identità. Legata allo sconto iperbolico è la tendenza a sottoassicurarsi contro certi rischi (Kunreuther, 1984). In generale, gli individui possono esercitare coercizione su comportamenti futuri che limitano il proprio conseguimento della massima uti-

lità: le persone possono volersi proteggere ma, a causa di una mancanza di autocontrollo, non lo fanno, e optano invece per la gratificazione immediata. «La gente tende a sottovalutare gli effetti di cambi delle proprie condizioni e quindi erroneamente rivolge le proprie preferenze del momento al consumo anche per le preferenze future. Più che suggerire semplicemente che la gente predice erroneamente gusti futuri, questa proiezione deviata postula un percorso sistematico in queste errate previsioni che può condurre ad errori sistematici negli ambienti di scelte "dinamiche", scrivono Lowenstein *et* al. (2003, p. 2). In aggiunta, gli individui spesso soffrono di propensione all'ottimismo (Weinstein, 1989): la percezione errata che i propri rischi siano, a parità di condizioni, inferiori a quelli di altri individui. La propensione all'ottimismo ci può condurre a credere che altri, ma non noi, saranno soggetti a violazioni della *privacy*.

Ed ancora: gli individui si imbattono in difficoltà quando affrontano rischi cumulativi. Slovic (2000), per esempio, mostra come fumatori giovani si rendono conto dei rischi a lungo termine legati al fumo, ma non percepiscono perfettamente la relazione tra i bassi rischi di ciascuna sigaretta a se stante ed il loro effetto cumulativo. La difficoltà di fronteggiare rischi cumulativi riguarda la *privacy*, in quanto le nostre informazioni personali, una volta divulgate, possono rimanere nel domino pubblico a lungo, e da lì possono essere correlate ad altri dati personali. Il risultato è che il rischio legato al fornire frammenti di dati personali collegabili tra loro è maggiore della somma dei rischi singoli associati ad ciascun frammento di informazione.

Inoltre, è più facile fronteggiare azioni ed effetti che sono più vicini a noi in termini temporali. Azioni ed effetti nel futuro remoto sono difficili da mettere in risalto data la nostra limitata lungimiranza (Jehiel e Lilico, 2002). Questo fenomeno può influire anche sulle decisioni in materia di *privacy*, in quanto i costi della protezione della *privacy* possono essere immediati, ma i compensi possono essere invisibili (assenza di invasione) e differiti a tempi futuri.

Per riassumere: quando affrontiamo decisioni sulla *privacy* raramente disponiamo di tutti gli elementi per una scelta informa-

ta. Ma anche se li avessimo, avremmo difficoltà ad analizzarli in maniera accurata. E anche se fossimo capaci di analizzarli, potremmo ancora comportarci in maniera diversa dalla scelta ottimale. Per esempio, in presenza di un beneficio immediato (come potrebbe essere uno sconto sul prezzo di un bene da acquistare *online*, offerto in cambio dei dati personali del compratore), il consumatore potrebbe decidere di dare via i propri dati personali e dunque accettare il rischio di un costo molto maggiore, sebbene futuro e solo potenziale (come il danno subito per frodi della carta di credito dovute alla informazione rivelata in quell'occasione). Acquisti e Grossklags (2005) in uno studio preliminare condotto nel 2005 negli Stati Uniti, hanno mostrato come infatti l'incompletezza dell'informazione, la razionalità limitata, e una serie di deviazioni comporamentali sembrino influenzare il processo decisionale degli individui nel contesto della *privacy*. La conclusione è che anche offrendo all'individuo completo controllo sull'uso dei suoi dati personali, questi potrebbe prendere decisioni contrarie al suo stesso interesse.

5. - Conclusione: Economia della *privacy*, tecnologia, e iniziative normative

È la *privacy* un bene che va difeso a prescindere, o la sua utilità va bilanciata con quella di altri interessi, come il diritto all'informazione e l'interesse per la trasparenza? E se i diversi interessi vanno bilanciati, il mercato sta assolvendo questo compito? Dobbiamo promulgare più leggi? Creare nuove tecnologie? Informare meglio gli individui?

L'economia non può rispondere alla prima domanda, ma può aiutare a rispondere alle altre, offrendo strumenti per lo studio dei *trade-offs* che emergono in questioni di *privacy*.

L'evoluzione dell'economia della *privacy* dagli anni ottanta ad oggi dimostra una comprensione sempre più sofisticata delle relazioni tra pubblico e privato nel trattamento dei dati; ma mostra anche che è ancora aperto il dibattito sulla relazione tra *privacy*, tecnologia, ed iniziative normative come la Direttiva euro-

pea ed il Codice della *privacy* italiano. Gli economisti della scuola di Chicago che aprirono il dibattito negli anni ottanta non avrebbero incoraggiato interventi normativi a vasto raggio come la Direttiva europea. Ma la nuova economia della *privacy* ha messo in luce le molte difficoltà che, all'atto pratico, un mercato senza norme incontra nel produrre la combinazione ideale di protezione e diffusione di dati personali. Già Noam (1996) ammetteva che, anche in un'economia di mercato, la mancanza di informazione completa per l'individuo (e la difficoltà ad accedere a strumenti di protezione) fossero di ostacolo alla protezione della *privacy*. L'uso secondario di informazioni personali e le esternalità che questo comporta la possibile scarsa lungimiranza dei consumatori, insieme alla tendenza delle imprese in competizione a investire più che socialmente utile nel raccogliere informazioni sui consumatori, sono esempi di fattori che possono sbilanciare l'equilibrio tra diffusione e protezione dei dati personali a svantaggio dell'individuo.

Alcuni hanno proposto come soluzione l'attribuzione di diritti di proprietà sui dati personali all'individuo stesso, così da proteggere la *privacy* ma al tempo stesso favorire lo scambio volontario nel mercato dei dati personali. Queste proposte sono state criticate da posizioni opposte — quelle della scuola di Chicago e quelle, più recenti, di giuristi come Pamela Samuelson. Da un lato, Posner (1978) ritiene che diritti di proprietà sull'informazione vadano accordati solo quando tale informazione sia sviluppata con un costo (per cui il diritto di proprietà crea gli incentivi necessari per assorbire detto costo), e quando i costi di transazione non siano di impedimento. Nel caso di informazione personale, Posner ritiene che manchino entrambi i presupposti (per esempio, i costi di transazione nell'informazione personale sarebbero troppo alti se un'impresa dovessere richiedere a ciascun individuo il suo consenso a che i suoi dati personali siano passati da un'impresa ad un'altra). Dall'altro lato, Samuelson (2000) ha notato come un sistema di diritti di proprietà dei dati personali sarebbe all'atto pratico estremamente complesso, costoso, e dal profilo legale incerto. In genere, nota Samuelson, la proprietà di un bene porta con sè l'abilità di vende-

re tale bene ad altri. Nel caso dell'informazione personale, il consumatore che decide di passare i suoi dati ad un'altra parte non ha controllo sugli usi e scambi futuri che questa parte ne farà. Non avendo controllo sui possibili costi che potrebbero derivare dalle altrui transazioni future, al consumatore manca una base adeguata per decide il prezzo a cui "vendere" la propria informazione.

Eppure, per via della mancanza di incentivi economici adeguati e per via delle difficoltà incontrate dall'individuo nel processo decisionale nel campo della *privacy*, nemmeno l'uso di tecnologie di protezione per il momento ha dato i risultati sperati (Acquisti, 2004*a*). Applicando modelli di gratificazione immediata allo studio del processo di decisione in materia di *privacy*, si può mostrare perché anche individui preoccupati per la propria *privacy* finiscono per non proteggerla a causa di alterazioni psicologiche ben documentate nella letteratura dell'economia comportamentale.

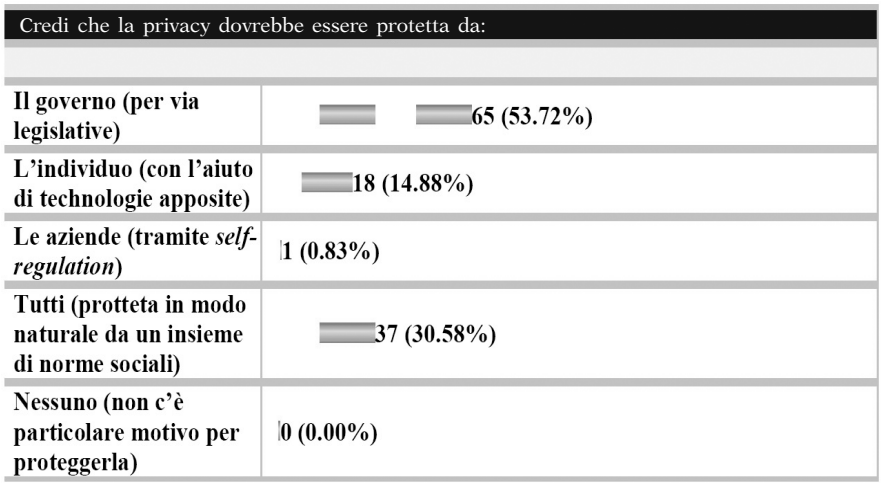
D'altra parte, iniziative legislative possono cercare di supplire alle difficoltà individuali, ma iniziative legislative nell'area della *privacy* possono diventare complicate, rapidamente obsolete, e, se numerose, anche contraddittorie, causando dunque gravi costi sociali (Samuelson, 2003).

È dunque possibile che le tecnologie di protezione, da sole, non possano risolvere il problema della *privacy* che altre tecnologie hanno creato, ma che neppure iniziative legislative, da sole, possano bilanciare i bisogni delle varie parti. Nel frattempo, i costi della *privacy* continuano a crescere: dallo *spam* al furto di identità (*Privacy* Rights Clearinghouse, 2000; Community Banker Association of Indiana, 2001; Federal Trade Commission, 2002; Gellman, 2002; Shostack, 2003; Odlyzko, 2003), e gli individui guardano ancora al governo e ad iniziative legislative per una protezione che il mercato non sembra offrire (Graf. 6).

Se da un punto di vista economico questo significhi che la *privacy* debba essere protetta a prescindere dalle risposte del mercato, è domanda ancora aperta. Ma nel tentare di rispondere a quella domanda, anche un approccio economico porta a concludere che il valore della *privacy* si estende oltre il regno delle ra-

GRAF. 6

OPINIONI SULLA RESPONSABILITÀ DELLA PROTEZIONE DELLA *PRIVACY*. CAMPIONE DI 119 INDIVIDUI ALLA CARNEGIE MELLON UNIVERSITY



Fonte: ACQUISTI A. - GROSSKLAGS J. (2005).

gioni finanziarie e dell'analisi dei costi e dei benefici, e finisce per dipendere da opinioni personali sull'importanza della libertà invidivuale e da visioni soggettive del tipo di società in cui ognuno di noi desidera vivere.

Breve guida all'economia della *privacy* su *Internet*

Proponiamo di seguito una lista di alcuni siti Internet da cui è possibile accedere ad ulteriori informazioni sull'economia della *privacy*.

1. *Alessandro Acquisti's Economics of Privacy*
http://www. heinz.cmu.edu/~acquisti/economics-privacy.htm
Una raccolta di *links* ad articoli, conferenze, organizzazioni, e siti di altri ricercatori dell'economia della *privacy*.

2. *Kai-Lung Hui's Privacy Page*
http://www.comp.nus. edu.s/iun/privacy.html
Il sito di un professore dell'Università Nazionale di Singapore, dedicato alla *privacy* e l'economia.

3. *Ross Anderson's Economics and Security Research Page*
http://www.ci.cani.ac.uk/users/rja14/econsec.html
Una pagina dedicata all'economia della sicurezza informativa.

4. *Roger Dingledine's Anonymity Bibliography*
http://freehaven. net/anonbib/topic.html
Una raccolta di articoli su *privacy* e anonimato, *focus* tecnologico.

5. *Jens Grossklags's EPrivacy Page*
http://www.sims.berkeley.edu/jens/resources/e-privacy.html
Una raccolta di articoli e risorse su *privacy* elettronica.

6. *Hal Varian's Information Economics Page*
http://www.sims.berkeley.edu/resources/infoecon/
Una delle risorse *Internet* più vaste sull'economia dell'informazione e dei sistemi informativi.

7. *Information Economics Page*
http://www. utdallas.edu/huseyin/security.html
Un'altra raccolta di *links* sull'economia della sicurezza informativa.

8. *UC Berkeley IGS's Financial Privacy Page*
http://www.is.berkeley.edu/library/htFinancial2003.html
Un sito presso l'Università di Berkeley, California, dedicato al tema della *privacy* dei dati finanziari.

9. *WEIS - Workshop on the Economics of Information Security*
http://infosecon.net/workshop/index.php
Il sito del *workshop* internazionale che dal 2002 raccoglie i lavori di studiosi nel ramo dell'economia della *privacy* e della sicurezza informativa.

10. *PET - Privacy Enhancing Technologies Workshop*
http://petworkshop.org
Il sito *Internet* di un *workshop* internazionale dedicato alle tecnologie della *privacy*, che accoglie anche contributi e articoli di carattere economico.

11. *EPIC - Electronic Privacy Information Center*
http://www.epic.org/
Un sito dedicato alle problematiche della *privacy* nella società dell'informazione.

12. *Privacilla*
http: //www.privacilla.org/
Un sito che discute dei problemi di *privacy* con un'impostazione libertaria ed in favore del libero mercato.

13. *Online Privacy Alliance*
http: //www.privacyalliance.org/
Il sito di un insieme di associazioni e compagnie che intendono promuovere iniziative di autoregolamentazione per la protezione della *privacy*.

14. *EFF - Electronic Frontier Foundation Privacy Page*
http://www.eff.org/Privacy/
Una serie di risorse dedicate alla protezione della *privacy* contro intrusioni e sorveglianza.

BIBLIOGRAFIA

ACQUISTI A., «*Privacy* and Security of Personal Information: Economic Incentives and Technological Solutions», *Workshop on Economics and Information Security (WEIS '02)*, 2002*a*.

— —, «Protecting *Privacy* with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments», *Workshop on Socially-informed Design of Privacy-enhancing Solutions, International Conference on Ubiquitous Computing (UBICOMP '02)*, 2002*b*.

— —, «Privacy and Security of Personal Information: Economic Incentives and Technological Solutions», in CAMP J. - LEWIS S. (eds.), *The Economics of Information Security,* 2004*a*.

— —, «Privacy in Electronic Commerce and the Economics of Immediate Gratification», *Proceedings of the ACM Conference on Electronic Commerce (EC '04)*, pp. 21-29, 2004*b*.

— —, «Note sull'economia della privacy», in CUFFARO V. - D'ORAZIO R. - RICCIUTO V. (eds.), *Il codice del trattamento dei dati personali*, Giappichelli, in corso di stampa.

ACQUISTI A. - DINGLEDINE R. - SYVERSON P., «On the Economics of Anonymity», *Financial Cryptography Conference (FC '03)*, Springer Verlag, LNCS 2742, pp. 84-102, 2003.

ACQUISTI A. - GROSSKLAGS J., «Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior», in CAMP J. - LEWIS S. (eds.), *The Economics of Information Security*, 2004.

— — - — —, «Privacy and Rationality in Decision Making», *IEEE Security Privacy,* January-February, pp. 24-30, 2005,.

ACQUISTI A. - VARIAN H. R., «Conditioning Prices on Purchase History», *Marketing Science,* vol. 24, n. 3, 1-15, presentato per la prima volta alla Haas School of Business IO Fest, UC Berkeley, Ottobre 2001, 2005.

ADAR E. - HUBERMAN B., «A Market for Secrets», *First Monday* 6(8).

AGRE P.E., «Introduction», in AGRE P. - ROTENBERG M. (eds.), *Technology and Privacy: The New Landscape*, Cambridge (MA), MIT Press, pp. 1-28, 1997.

AGRE P.E. - ROTENBERG M., *Technology and Privacy: The New Landscape*, Cambridge (MA), MIT Press, 1997.

AKERLOF G.A., «The Market for "Lemons": Quality Uncertainty and the Market Mechanism», *Quarterly Journal of Economics,* vol. 84, n. 3, pp. 488-500, 1970.

BELLOTTI V., «Design for Privacy in Multimedia Computing and Communications Environments», in AGRE P. - ROTENBERG M. (eds.), *Technology and Privacy: The New Landscape*, MIT Press, pp. 63-98, 1997.

BENALOH J.C., *Verifiable Secret-ballot Elections*, PhD Thesis, Yale University, Department of Computer Science, Number 561, 1987.

BENALOH J.C. - YUNG M., «Distributing the Power of a Government to Enhance the Privacy of Voters», *ACM Symposium on Principles of Distributed Computing*, pp. 52-62, 1986.

BLATTBERG R.C. - DEIGHTON J., «Interactive Marketing: Exploiting the Age of Addressability», *Sloan Management Review,* vol. 33, n. 1, pp. 5-14, 1991.

BLOUSTEIN E.J., «Privacy as an Aspect of Human Dignity - An Answer to Dean Prosser», *New York University Law Review,* vol. 39, pp. 962-1007, 1964.

BRASSARD G. - CREPEAU C. - ROBERT J.M., «All-ornothing Disclosure of Secrets», *Advances in Cryptology (Crypto '86)*, Springer Verlag, LNCS 263, pp. 234-238, 1987.

BRIN D., *The Transparent Society*, Addison Wesley, Reading, 1998.

BRUNK B.D., «Understanding the Privacy space», *First Monday,* vol. 7, n. 10. *http:// www.firstmonday. org/issues/issue7_1O/brunk/ index. html*, 2002.

CALZOLARI G. - PAVAN A., «Optimal Design of Privacy Policies», *Technical Report*, Gremaq, University of Toulouse, 2001.

CAMENISCH J. - LYSYANSKAYA A., «An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation», *Advances in Cryptology (Eurocrypt '01)*, Springer Verlag, LNCS 2045, pp. 93-118. *http:// www.citeseer.nj.nec.com/camenischOlefficient.html*, 2001.

CANNY J., *Trust and Risk in Internet Commerce*, MIT press, 2000.

— —, «Collaborative Filtering with Privacy Via Factor Analysis», *Sigir '02.*

CHAUM D., 1981, «Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms», *Communications of the ACM* vol. 24, n. 2, 84-88, 2002.

— —, «Blind Signatures for Untraceable Payments», *Advances in Cryptology (RYPTO '82)*, Plenum Press, pp. 199-203, 1983.

— —, «Security Without Identification: Transaction Systems to Make big Brother Obsolete», *Communications of the ACM*, vol. 28, n. 10, pp. 1030-44, 1985.

CHAUM D. - EVERTSE J.H., «A Secure and privacy Protecting Protocol for Transmitting Personal Information Detween Organizations», *Advances in Cryptology (Crypto '86)*, pp. 118-67, 1985.

CHAUM D. - VAN HEJIST E., «Group Signatures», *Advances in Cryptology (Eurocrypt '91),* Springer Verlag, LNCS 547, pp. 257-65, 1991.

CLARKE R., «Internet Privacy Concerns Confirm the Case for Intervention», *Communications of the ACM,* vol. 42, n. 2, pp. 60-7, 1999.

COMMUNITY BANKER ASSOCIATION OF INDIANA, «Identity Fraud Expected to Triple by 2005», *http://www.cbai.org/Newsletter/December2001/identity_fraud_de2001. htrn.*

COREY S., «Professional Attitudes and Actual Behavior», *Journal of Educational Psychology*, vol. 28, n. 1, 271-80, 2001.

DIAZ C. - SEYS S. - CLAESSENS J. - PRENEEL B., «Towards Measuring Anonymity», *Privacy Enhancing Technologies Workshop (PET '02)*, 2002.

EBUSINESSFORUM, «The Great Online Privacy Debate», *http://www. ebusinessforum. corn/index. asp?doc_ id=1785&layout=rich_story*, 2000.

EUROPEAN PARLIAMENT, «Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data», *http://www.europa.eu.int/comm/ internal_rnarket/en/dataprot/law/.,* 1995.

— —, «Privacy Online: Fair Information Practices in the Electronic Marketplace», *http://www.ft.gov/reports/privacy2000/privacy2000.pdf.*

— —, «FTC Testifies on Identity Theft and the Impact on Seniors» *http://www.ftc.gov/opa/2002/07/senioridtheft.htm.,* 2002.

FRIEDMAN E.J. - RESNICK, P., «The Social Cost of Cheap Pseudonyms», *Journal of Economics and Management Strategy*, vol. 10, n. 2, pp. 173-99, 2001.

FROOMKIN A.M., «The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution», *University of Pennsylvania Law Review,* vol. 143, pp. 709-895, 1995.

FROOMKIN A.M., «The Death of Privacy?», *Stanford Law Review,* vol. 52, pp. 1461-43, 2000.

GARFINEKL S., *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, 2000.

GELLMAN R., «Privacy, Consumers, and Costs - How the Lack of Privacy Costs Consumers and why Business Studies of Privacy Costs are Biased and Incomplete», *http://www. epic.org/report si dmf privacy.html.*, 2002.

GOLDBERG I.A., «A Pseudonymous Communications Infrastructure for the Internet», Ph.D. Thesis, University of California at Berkeley, 2000.

GOLDSCHLAG D. - REED M. - SYVERSON P., «Onion Routing for Anonymous and Private Internet Connections», *Communications of the ACM,* vol. 42, n. 2, pp. 39-41, 1999.

GOODLATTE B., *Statement at the Privacy in the Digital Age Hearing before the Subcommittee on the Constitution, Federalism and Property Rights of the Committee on Judiciary Unites States Senate*, 105h Congress, March 17, 1998.

GRIMALDI J., «Zoo won't Release Medical Records Privacy Cited», *Washington Post,* May 7, 2002.

HIRSHLEIFER J., «The Privacy and Social Value of Information and the Reward to Inventive Activity», *American Economic Review,* vol. 61, pp. 561-74, 1971.

— —, «Privacy: Its Origins, Function and Future», *Journal of Legal Studies,* vol. 9, pp. 649-64, 1980.

JEHIEL P. - LILICO A., «Smoking Today and Stopping Tomorrow: A Limited Foresight Perspective», *Technical report*, Department of Economics, UCLA, 2002.

JIANG X. - HONG J. I. - LANDAY J.A., «Approximate Information Flows: Socially Based Modeling of Privacy in Ubiquitous Computing», *International Conference on Ubiquitous Computing (Ubicomp '02)*, Springer Verlag, LNCS 2498, 2002.

JONES V.E. - CHING N. - WINSLETT M., «Credentials for Privacy and Interoperation», *Proceedings of the New Security Paradigms Workshop, http://www. drl.cs.uiuc.edu/security/pubs.html*, 1995.

JUPITER RESEARCH, «Seventy Percent of US Consumers Worry About Online Privacy, but Few Take Protective Action», *http://www.jmm.com/xp/jmm/press/2002/pr.060302. xml*, 2002.

KAHNEMAN D. - TVERSKY A., *Choices, Values, and Frames,* University Press, Cambridge, 2000.

KUNREUTHER H., «Causes of Underinsurance Against Natural Disasters», *Geneva Papers on Risk and Insurance* (31), 1984.

LAPIERE R., «Attitudes versus actions», *Social Forces*, vol. 13, n. 2, pp. 230-37, 1934.

LAUDON K.C., «Markets and Privacy», *Communications of the ACM,* vol. 39, n. 9, pp. 92-104, 1996.

LESSING L., *Code and Other Laws of Cyberspace*, Basic Books, 1999.

LITMANN J., «Information Privacy-Information Property», *Stanford Law Review*, vol. 52, n. 1283, 2000.

LOWENSTEIN G. - O'DONOGHUE T. - RABIN M., «Projection bias in Predicting Future Utility», *Technical Report*, Carnegie Mellon University, Cornell University, and University of California, Berkele, *http://www.econwpa.wustl.edu/eps/get/papers/0012/0012003.pdf.*, 2003.

LUNDBLAD N., «Privacy in a Noise Society», *http://www.sics.se/privacy/wholes2004/papers/lundblad.pdf.*

MURPHY R.F., «Social Distance and the Veil», *American Anthropologist,* vol. 66, n. 6, pp. 1257-74, 1964.

MUTI A., «La legge c'è, va rispettata», *Libero News,* March 9, *http://www. news2000. libero.it/speciali/sp148/pgl.html*, 2004.

NOAM E.M., «Privacy and Self-regulation: Markets for Electronic Privacy», *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, 1996.

ODLYZKO A., «Privacy, Economics, and Price Discrimination on the Internet», *Fifth International Conference on Electronic Commerce*, ACM, pp. 355-66, 2003.

O'DONOGHUE T. - RABIN M., «Choice and Procrastination», *Quartely Journal of Economics,* vol. 116, n. 1, pp. 121-60, 2001.

PNG I. - HANN I.H. - HUI K.L. - LEE T.S., *Direct Marketing: Privacy and Competition*, Mimeo, 2003.

POSNER R.A., «An Economic Theory of Privacy», *Regulation*, May-June, pp. 19-26, 1978.

— —, «The Economics of Privacy», *American Economic Review,* vol. 71, n. 2, pp. 405-09, 1981.

PRIVACY RIGHTS CLEARINGHOUSE, «Nowhere to Turn: Victims Speak out on Identity Theft», *http://www.privacyrights.org/an idtheft2000.htm,* 2000.

PROSSER W., «Privacy», *California Law Journal,* vol. 48, n. 2, pp. 383-423, 1960.

RABIN M. - O'DONOGHUE T., «The Economics of Immediate Gratification», *Journal of Behavioral Decision Making,* vol. 13, n. 2, pp. 233-50, 2000.

REGAN P.M., *Legislating Privacy*, The University of North Carolina, Chapel Hill, 1995.

REIDENBERG J.R., «Setting Standards for fair Information Practice in the U.S. Private Sector», *Iowa Law Review,* pp. 497-551, 1995.

REITER M.K. - RUBIN A.D., «Anonymous web Transactions with Crowds», *Communications of the ACM,* vol. 42, n. 2, pp. 32-38, 1999.

RUBIN P.H. - LENARD T.M., «Privacy and the Commercial use of Personal Information», *Technical Report*, The Progress Freedom Foundation, Washington, DC, USA, 2002.

SAMUELSON P., «Privacy as Intellectual Property», *Stanford Law Review*, vol. 52, n. 1125, 2000.

— —, «The Social Costs of Inchoerent Privacy Policies», *Presentation* at IBM Almaden Privacy Institute, 2001.

SCHOEMAN F., «Privacy: Philosophical Dimensions», *American Philosophical Quarterly,* 21.

SCOGLIO S., *Transforming Privacy: A Transpersonal Philosophy of Rights*, Praeger, Westport, 1998.

SERJANTOV A. - DANEZIS G., «Towards an Information the Oretic Metric for Anonymity», *Privacy Enhancing Technologies Workshop (PET '02)*, 2002.

SHOSTACK A., «Paying for Privacy: Consumers and Infrastructures», *Workshop on Economics and Information Security (WEIS '03)*, 2003.

SIMON H.A., *Models of bounded rationality*, MIT Press, Cambridge, MA, 1982.

SLOVIC P., «What does it Mean to Know a Cumulative Risk? Adolescents' Perceptions of Short-term and Long-term Consequences of Smoking», *Journal of Behavioral Decision Making,* vol. 13, pp. 259-66, 2000.

SMITH R.E., *Ben Franklin's web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Sheridan Books, 2000.

SPIEKERMANN S. - GROSSKLAGS J. - BERENDT B., «E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior», *Proceedings of the ACM Conference on Electronic Commerce (EC '01)*, pp. 38-47, 2001.

STATEN M.E. - CATE F.H., «The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA», *Duke Law Journal*, vol. 52, pp. 745-85, 2003.

STEWART B., «Privacy Impact Assesments», *Privacy Law and Policy Reporter,* 39.

STIGLER G.J., «An Introduction to Privacy in Economics and Politics», *Journal of Legal Studies,* vol. 9, pp. 623-44, 1980.

STREIFIELD D., «On the Web Price Tags Blur: What you Pay Could Depend on Who you Are», *The Washington Post,* September, 27, 2001.

SWEENEY L., «k-anonymity: A model for Protecting Privacy», *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* vol. 10, n. 5, pp. 557-570, 2002.

SWIRE P.P. - LITAN R.E., *None of Your Business*, Brookings Institution Press, Washington, DC, 1998.

TANG Z. - HU Y.J. - SMITH M., «Protecting Online Privacy: Self-regulation, Mandatory Standards, or Caveat Emptor», *http:www.//ssrn.com/abstract=555878,* 2004.

TAYLOR C.R., «Consumer Privacy and the Market for Customer Information», *Rand Journal of Economics*, vol. 35, n. 4, pp. 631-51, 2004*a*.

— —, «Privacy and Information Acquisition in Competitive Markets», *Technical report*, Duke University, Economics Department, 03-10, 2004*b*.

TURKINGTON R., «Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy», *Northern Illinois University Law Review*, vol. 10, 479-520, 1990.

VARIAN H.R., «Economic Aspects of Personal Privacy», *Privacy and Self-regulation in the Information Age*, National Telecommunications and Information Administration, 1996.

VARIAN H.R. - SHAPIRO C., *US Government Information Policy*, Presented at Highlands Forum, Department of Defense, June 8, Washington DC, 1997.

WARE W.H., «Emerging Privacy Issues», *Technical Report*, *Rand Paper Series*, 1985.

WARREN S. - BRANDEIS L., «The Tight to Privacy», *Harvard Law Review*, vol. 4, n. 5, pp. 193-220, 1890.

WEINSTEIN N.D., «Optimistic Biases About Personal Risks», *Science*, vol. 24, pp. 1232-33, 1989.

WESTIN A.F., *Harris-Equifax Consumer Privacy Survey 1991*, Equifax Inc., Atlanta, (GA).

— —, *Privacy and Freedom*, Atheneum Publishers, New York, 1967.

WHITE A., «Privacy Groups Slam new EU Directive», *ElectricNews.net*, May 31, 2002.

WHITTEN A. - TYGAR J.D., «Why Johnny can't Encrypt: A Usability Evaluation of PGP 5.0», *8th USENIX Security Symposium*, 1999.

WINSBOROUGH W.H. - SEAMONS K.E. - JONES V.E., «Automated Trust Negotiation», *Darpa Information Survivability Conference and Exposition*, *http://drl.Cs.uiuc.edu/security/pubs. html*, 2000.

ZETTELMEYER F. - MORTON F.M.S. - SILVA-RISSO J., «Cowboys or Cowards: Why are Internet Car Prices Lower?», *Technical Report*, Haas School, UC Berkeley Marketing, *Working Paper,* No. 01-1, 2001.