Diritto, Economia e Tecnologie della Privacy

Anno I, Numero Unico, 2010

Istituto Italiano Privacy

Diritto, Economia e Tecnologie della Privacy

Anno I, numero unico, 2010
Registrazione al Tribunale di Arezzo n. 1P/10RS del 26 ottobre 2010
Rivista quadrimestrale

Direzione e redazione: via Boezio, n. 6, 00195, Roma; Direttore responsabile: Giovanni Crea

Proprietà della rivista: Istituto Italiano per la Privacy. Consiglio di Amministrazione dell'Istituto Italiano per la Privacy: Luca Bolognini - Presidente; Diego Fulco - Direttore; Pietro Paganini - Consigliere; Paolo Balboni - Consigliere.

Editore: Istituto Italiano per la Privacy, via Boezio, n. 6, 00195, Roma
www.istitutoitalianoprivacy.it
info@istitutoitalianoprivacy.org
tel.: 06 32803406
fax: +39 06 23328983

Condizioni economiche

- singolo numero: € 25, 00
- abbonamento annuale (tre numeri): € 70,00 (L'abbonamento decorre dal mese di gennaio di ciascun anno. La sottoscrizione dell'abbonamento nel corso dell'anno dà diritto a ricevere i numeri arretrati). Il pagamento può essere effettuato mediante versamento bancario sul conto intestato a Istituto Italiano per la Privacy – IBAN – IT75C0316501600000110403686

INDICE

Editoriale

La rivista "Diritto, Economia e Tecnologie della Privacy" nasce in seno all'Istituto Italiano per la Privacy, dalla sua forte convinzione di poter contribuire, anche attraverso un mezzo editoriale, a diffondere una cultura della materia che sia multidisciplinare e che, per questo, possa integrare i punti di vista di giuristi, economisti, esperti di nuove tecnologie, senza tuttavia escludere il contributo di studiosi di altre discipline, di figure appartenenti al mondo imprenditoriale, alle istituzioni, alle categorie professionistiche. E ciò per il semplice fatto che, oltre alla considerazione che la riservatezza dei dati personali è un interesse legittimato da un diritto, tali dati sono anche indispensabili in economia, e perché – nel bene e nel male – anche la tecnologia c'entra, non fosse altro per l'affermarsi delle ICT (Information and communications technologies); nel bene perché le generazioni Pet (privacy enhancing technologies) e Pbd (privacy by design) si offrono come braccio tecnologico del diritto; nel male in quanto le predette soluzioni non sono ancora diffuse e, nell'attesa che lo siano, la Rete resta sede di pratiche di profiling occulte, poste in essere con appositi ritrovati tecnologici. E, ancora, perché l'esperienza di un'impresa, la posizione di un'autorità o il punto di vista di un professionista possono farci «vedere» il problema sotto aspetti più pratici.

Nell'ambiente tecnologico/digitale, affrontare le questioni della privacy, come di altri temi che in esso si ripropongono – gli scambi commerciali, la protezione dei minori, la circolazione dei contenuti d'autore, per fare alcuni esempi – richiede un approccio diverso, che tiene conto delle mutate condizioni. Ed è secondo questa prospettiva che la rivista si propone ai suoi futuri lettori. Per intenderci, si tratta del fatto che una parte delle attività dell'uomo si trasferirà in Rete; e che in tale «spazio» molte questioni di privacy andranno affrontate e risolte anche a colpi di regolazione tecnica. Chiari segnali in tal senso sono le questioni di equilibrio che si pongono quando, anche in Internet, l'esigenza della privacy si incontra con interessi di pari dignità; qui, il conflitto con la proprietà intellettuale, con le esigenze

di giustizia e con la libertà di informazione va dunque gestito con opportuni bilanciamenti che è bene che vengano realizzati anche ricorrendo a misure tecnologiche. Anche le soluzioni di cloud computing, che gli internet service provider si apprestano ad adottare per motivi di efficienza, pongono nuove questioni sul fronte della protezione dei dati personali; la «nuvola» evoca un'immagine di dispersione che porta naturalmente a domandarsi come, in tale condizione, gli interessati potrebbero controllare il trattamento dei dati che li riguardano. E che dire dei metodi utilizzati da taluni provider per accedere ai dati personali, sulla cui conformità al principio della trasparenza è plausibile avanzare qualche riserva; sotto questo aspetto, i recenti casi RapLeaf e Google Street View sono, a dir poco, preoccupanti se si considera che, come sembra, entrambe le società avrebbero svolto la raccolta di dati personali all'insaputa degli interessati, privando questi della condizione di poter esercitare, anche ex post, il diritto di opposizione. Peraltro, è anche vero che il trattamento dei dati personali ha una giustificazione economica, sia perché questa attività è realisticamente parte integrante del processo produttivo delle imprese, obbligate ad adeguarsi alla "legge della differenziazione del prodotto", sia in ragione degli effetti di ritorno sui consumatori valutabili in termini di soddisfazione dei loro bisogni e desideri che – neppure a dirlo – sono personali; e questo è tanto più vero nella prospettiva di un'economia che fa uso di reti e servizi di comunicazione elettronica, in cui offerte e pubblicità di beni sono sempre più attagliate sulle caratteristiche dei singoli piuttosto che dei gruppi. Al riguardo, non può dirsi che il legislatore comunitario – se pure con estrema cautela – non abbia dato prova di attenzione per il fronte economico, con la previsione di norme più flessibili per un trattamento trasparente dei dati personali. Non fosse altro per coerenza con l'obiettivo del mercato unico; ma anche perché – e qui la motivazione è sotto gli occhi di tutti – le imprese che, per ragioni di efficienza e di efficacia, operano per contatto diretto con i consumatori sono una realtà economica non più trascurabile, la cui attività si caratterizza per l'uso di almeno un set minimo di dati personali (coordinate telefoniche o di posta elettronica e dati anagrafici).

Tra i contenuti della rivista, non poteva mancare una sezione giuridica in cui riportare provvedimenti e casi di particolare interesse. Non è certo un'innovazione, ma non va nemmeno considerata una scelta banale; la finestra giuridica è imprescindibile per uno strumento editoriale che si propone di fornire un quadro strutturato sulla privacy nella società dell'informazione, che dunque – oltre ai contributi su argomenti e accadimenti – includa anche l'attività giuridica. E, anzi, in un contesto dinamico, quale è la transizione verso la «network society», di tale attività vanno seguiti gli sviluppi. Sotto questo profilo, è interessante comprendere, ad esempio, l'atteggiamento del diritto di fronte all'evoluzione tecnologica; tema non di poco rilievo, su cui il dibattito sta convergendo auspicando, sia pure con qualche punta di scetticismo, che le regole possano indirizzare l'industria delle tecnologie verso soluzioni che possano tutelare i diritti fondamentali.

Questa rivista inizia la sua esperienza – neppure a dirlo – con entusiasmo e voglia di crescere. Le idee non mancano, e di queste se ne darà evidenza nei prossimi numeri, ben inteso con la disponibilità della redazione e dell'Istituto Italiano per la Privacy a raccogliere contributi ma anche suggerimenti e critiche per migliorare la nostra produzione scientifica.

La privacy nel mercato europeo delle comunicazioni elettroniche: cosa cambia dopo la direttiva 2009/136/CE di riforma della direttiva 2002/58/CE sulla tutela dei dati personali nel settore delle comunicazioni elettroniche.

Alessandro del Ninno [*]

SOMMARIO: 1. Introduzione: la riforma del mercato europeo delle comunicazioni elettroniche – 2. I principali punti della riforma del mercato europeo delle comunicazioni elettroniche – 3. La tutela della vita privata nel settore delle comunicazioni elettroniche alla luce della nuova direttiva 2009/136/CE – 3.1 Le nuove norme in materia di sicurezza dei trattamenti – 3.2 Le informazioni raccolte nei riguardi dell'abbonato o dell'utente – 3.3 Le modifiche alla disciplina sulle comunicazioni indesiderate – 3.4 Conclusioni: rinvio alle modifiche dell'impianto sanzionatorio.

1. Introduzione: la riforma del mercato europeo delle comunicazioni elettroniche.

Il 18 Dicembre 2009 sono definitivamente entrate in vigore le norme del nuovo *"Pacchetto Telecom"* che dopo un travagliato percorso di approvazione (la prima proposta di riforma, ad opera della Commissione europea, risale al 2007) consentiranno ad oltre 500 milioni di cittadini europei, grazie a una concorrenza più forte sul mercato europeo delle telecomunicazioni, più ampie possibilità di scelta, una copertura più estesa di connessioni internet in banda larga in tutta Europa e una maggiore protezione della vita privata nei confronti degli operatori di telecomunicazioni. La riforma – che dovrà essere implementata nelle legislazioni nazionali degli Stati Membri comunque entro il mese di Giugno 2011 (con diverse scadenze per le varie direttive) – ha aggiornato, anche dal punto di vista degli sviluppi

[*] Avvocato, Responsabile del Dipartimento ICT & Internet Law dello studio legale Tonucci & Partners; Istituto Italiano per la Privacy.

tecnologici intervenuti nel frattempo[1], il precedente pacchetto di direttive che già nel 2002 aveva introdotto un rilevante quadro europeo omogeneo nel settore delle comunicazioni elettroniche[2]. Alle nuove direttive[3] – ed a completamento della riforma – si affianca inoltre un regolamento comunitario (immediatamente applicabile negli ordinamenti nazionali e già in vigore) che istituisce la nuova autorità europea per le telecomunicazioni, denominata "*Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC)*"[4]. La

[1] Ad esempio, nelle direttive del 2002 non venivano adeguatamente regolamentate la telefonia *voice-over-IP* (VOIP) o la prestazione di servizi televisivi mediante banda larga.

[2] Il precedente "*Pacchetto Telecom*" era costituito da cinque direttive: la direttiva 2002/19/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate (*direttiva accesso*); la direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica e all'interconnessione delle medesime (*direttiva autorizzazioni*); la direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (*direttiva quadro*); la direttiva 2002/22/CE (*direttiva servizio universale*) e la direttiva 2002/58/CE (*direttiva relativa alla vita privata e alle comunicazioni elettroniche*).

[3] Cioè la direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 (G.U.C.E. n. L 337 del 18/12/2009 pag. 0037 – 0069), nota anche come "*Better Regulation Directive*", recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica e la direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 (G.U.C.E. n. L 337 del 18/12/2009 pag. 0011 - 0036), nota anche come "*Citizens' Rights Directive*" recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

[4] Regolamento (CE) n. 1211/2009 del Parlamento europeo e del Consiglio del 25 novembre 2009 che istituisce l'Organismo dei regolatori europei delle

nuova autorità europea per le telecomunicazioni (formata dai presidenti delle 27 autorità regolatrici nazionali delle telecomunicazioni) presterà assistenza ai regolatori nazionali delle telecomunicazioni ed alla Commissione europea per garantire che i servizi del settore (e il relativo quadro normativo) siano offerti in modo coerente ed a condizioni di effettiva concorrenza in tutto il territorio dell'Unione europea, rafforzando così il mercato unico delle telecomunicazioni.

2. I principali punti della riforma del mercato europeo delle comunicazioni elettroniche.

Per comprendere appieno il nuovo quadro normativo in cui si innesta anche la modifica della direttiva 2002/58/CE sulla tutela della privacy nelle comunicazioni elettroniche, può essere opportuno ricordare le linee portanti della riforma approvata, che la stessa Commissione europea ha riassunto in 12 punti: 1) il diritto dei consumatori europei a cambiare, in 1 giorno lavorativo, il proprio operatore di telefonia fissa o mobile mantenendo il proprio numero di telefono; 2) una migliore informazione dei consumatori atta ad accrescerne la consapevolezza nel momento in cui si sottoscrivono i servizi; 3) la protezione del nuovo e codificato diritto dei cittadini europei di accedere alla rete Internet (e sul punto – proposto come emendamento dal Parlamento Europeo nell'ambito della procedura di co-decisione legislativa – si è quasi arrivati allo scontro istituzionale con il Consiglio e la Commissione); 4) nuove garanzie per una rete più aperta e "neutrale"; 5) la tutela dei consumatori contro le violazioni dei dati personali e contro la posta elettronica indesiderata (*spam*); 6) un migliore accesso ai servizi di emergenza tramite il numero unico europeo 112; 7) la maggiore autonomia e indipendenza delle autorità di regolazione nazionale nel settore delle telecomunicazioni; 8) l'istituzione di una nuova Autorità europea per le telecomunicazioni

---

comunicazioni elettroniche (BEREC) e l'Ufficio (G.U.C.E. n. L 337 del 18/12/2009 pag. 0001 – 0010).

che aiuterà a garantire una concorrenza leale e più coerenza della regolamentazione nei mercati delle telecomunicazioni; 9) il rafforzamento del potere della Commissione UE di sovrintendere a misure regolamentari proposte dalle autorità nazionali di controllo; 10) la possibilità di imporre come ultimo rimedio la separazione funzionale tra reti e servizi di comunicazione elettronica come mezzo per superare i problemi di concorrenza; 11) l'accelerazione ed il potenziamento della banda larga in tutta Europa; 12) il potenziamento della concorrenza e degli investimenti nelle reti di accesso di prossima generazione. I consumatori europei godranno dunque di nuovi o rafforzati diritti, come il diritto di cambiare operatore di telefonia mobile o fissa entro un giorno lavorativo mantenendo il proprio numero, il diritto ad una migliore informazione sui servizi a cui si abbonano e il diritto di essere informati delle violazioni dei dati personali da parte dei loro operatori di telecomunicazioni. Gli operatori dovranno inoltre dare agli utenti la possibilità di sottoscrivere un contratto di durata non superiore a 12 mesi. In base alle nuove norme UE i regolatori nazionali avranno inoltre il potere di stabilire livelli minimi di qualità dei servizi di trasmissione in rete in modo da promuovere la "neutralità della rete" a favore dei cittadini europei. La riforma del settore delle telecomunicazioni riafferma e rafforza i diritti fondamentali dei consumatori europei per quanto riguarda l'accesso alla Rete Internet. Una nuova disposizione sulla libertà di Internet, inserita nel pacchetto di misure su insistente richiesta del Parlamento europeo, precisa che tenendo conto dei diritti fondamentali di cui godono i cittadini europei, tra cui il diritto alla protezione della vita privata, le autorità nazionali potranno restringere l'accesso a Internet per motivi di interesse pubblico solo dopo l'espletamento di una procedura preliminare equa e imparziale e dopo un controllo giurisdizionale efficace e tempestivo.

3. La tutela della vita privata nel settore delle comunicazioni elettroniche alla luce della nuova direttiva 2009/136/CE.

La direttiva 2009/136/CE (nel prosieguo "Direttiva") copre in realtà tre diversi ambiti. Da un lato, difatti, modifica la precedente direttiva

"*Servizio Universale*" 2002/22/CE ed i relativi diritti degli utenti in materia di reti e di servizi di comunicazione elettronica; dall'altro reca modifiche al regolamento 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori. Il terzo ambito – che è quello che qui interessa ai fini della presente analisi – è infine quello della riforma della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Tale direttiva continua ad essere in vigore con le integrazioni e modifiche appunto introdotte dalla Direttiva in esame.

Se le modifiche introdotte dalla Direttiva all'articolo 1 della direttiva del 2002 si limitano a precisare che l'ambito della tutela armonizzata riguarda – oltre alla protezione della "*vita privata*" – anche quella del "*diritto alla riservatezza*", già l'analisi delle modifiche all'articolo 2 fa comprendere il diverso approccio riformatore. Difatti, la Direttiva – dopo aver modificato la definizione di "*dati relativi all'ubicazione*" aggiungendo alla previgente definizione che sono tali non solo i dati trattati in una rete di comunicazione elettronica, ma anche quelli trattati "*da un servizio di comunicazione elettronica*" che indichi la posizione geografica dell'apparecchiatura terminale dell'utente (ed è noto quanto dal 2002 si siano esponenzialmente ampliati e diffusi i cosiddetti servizi di geolocalizzazione) – introduce una nuova lettera all'articolo 2 recante la definizione di "*violazione dei dati personali*". E' tale la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella Comunità.

E' interessante notare come tale norma ricolleghi ad una qualsivoglia violazione delle misure a garanzia della sicurezza delle reti e delle informazioni una automatica violazione dei dati personali. Come specificato dal Considerando n. 53 della Direttiva, una rete o un sistema di informazione mediante i quali avviene il trattamento dei dati relativi al traffico su una rete di comunicazione elettronica dovrebbero avere la capacità di resistere ad eventi accidentali o azioni illecite o dolose (ad esempio: accesso non autorizzato alle reti di

comunicazioni elettroniche, distribuzione dolosa di codici, attacchi finalizzati al diniego di servizi, danni ai computer o ai sistemi di comunicazione elettronica) che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi. Le violazioni di sicurezza sono dunque qualificate automaticamente dalla Direttiva come violazioni dei dati personali.

Ancor più significativa è la modifica dell'articolo 3 della direttiva 2002/58: la nuova Direttiva amplia infatti i servizi interessati dalla nuova disciplina. Se l'ambito di applicazione era prima quello del "*trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità*"[5], è ora interessante notare che tale ambito è esteso dalla Direttiva anche alle "*reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati*". Ad esempio, in considerazione del progresso tecnologico intervenuto in questi anni che ha permesso lo sviluppo di nuove applicazioni basate su dispositivi per la raccolta e l'identificazione dei dati, come ad esempio i dispositivi senza contatto che utilizzano le radiofrequenze (i *Radio Frequency Identification Devices* - RFID), la Direttiva dispone che quando tali dispositivi sono collegati a reti di comunicazione elettronica accessibili al pubblico, o usano servizi di comunicazione elettronica come infrastruttura di base, a tale ambito siano estese le disposizioni pertinenti della direttiva 2002/58/CE, in particolare quelle sulla sicurezza, sui dati relativi al traffico e alla localizzazione e sulla riservatezza.

3.1. Le nuove norme in materia di sicurezza dei trattamenti.

Particolarmente significative sono le modifiche e le integrazioni che la Direttiva apporta all'articolo 4 della direttiva 2002/58. Tali modifiche incidono positivamente sul rafforzamento delle misure di sicurezza nei relativi trattamenti (e non a caso la stessa rubrica dell'articolo 4 – "*Sicurezza*" – è modificata in "*Sicurezza del trattamento*"). Lo scopo perseguito dalle nuove norme è quello di far

[5] Rimane invariata, anche alla luce delle modifiche, la previsione della non applicabilità della disciplina in esame ai gruppi chiusi di utenti né alle reti aziendali.

sì che un fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotti misure tecniche e organizzative adeguate per assicurare la sicurezza dei suoi servizi, oltre quelle già previste dalla Direttiva europea sulla tutela dei dati personali[6]. Tali misure ulteriori devono assicurare che i dati personali siano accessibili soltanto al personale autorizzato per scopi legalmente autorizzati e che i dati personali conservati o trasmessi nonché la rete e i servizi siano protetti. È altresì assai interessante l'introduzione dell'obbligo per i fornitori di strutturare una politica generale di sicurezza per il trattamento dei dati personali onde individuare le vulnerabilità dei sistemi e mettere in atto regolarmente misure di monitoraggio, di prevenzione, di correzione e di attenuazione. A tale obbligo per i fornitori è collegato il potere delle autorità nazionali competenti di "*verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e di emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire*".

Se si effettua una comparazione delle nuove norme in materia di sicurezza nei trattamenti introdotte dalla Direttiva con quelle già vigenti – ad esempio – nella normativa italiana sulla protezione dei dati personali[7], emerge che nell'ordinamento italiano alcuni dei nuovi obblighi risultano già implementati. Ai sensi dell'art. 32 del Codice della privacy – difatti – il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve già adottare idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita. Inoltre, sempre ai sensi del citato articolo, quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di

[6] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (G.U.C.E. n. L 281 del 23/11/1995 pag. 0031 – 0050).

[7] D.lgs. 30 Giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, in G.U. n. 174 del 29 luglio 2003, s.o. n. 123.

comunicazione elettronica accessibile al pubblico deve adottare tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni (e in caso di mancato accordo la norma prevede che, su richiesta di uno dei fornitori, la controversia sia definita dall'Autorità per le garanzie nelle comunicazioni). Infine, l'articolo 32 del Codice della privacy impone ai fornitori obblighi di specifica informativa, prevedendo di informare gli abbonati e, ove possibile, gli utenti, se sussista un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare, tutti i possibili rimedi e i relativi costi presumibili[8]. Si può ritenere che l'articolo 32 del Codice della privacy già contenga le misure richieste dalla Direttiva. Inoltre, l'obbligo di strutturare una politica generale di sicurezza potrebbe essere altresì in una certa misura già implementato se si considerano le norme del Codice della privacy e del Disciplinare Tecnico – Allegato B al Codice sulle misure minime e idonee di sicurezza.

Ciò che appare del tutto nuovo è l'insieme di obblighi informativi successivi (ad una violazione di sicurezza) che la Direttiva impone ai fornitori di servizi di comunicazione elettronica. Se si guarda sempre al Codice della privacy, attualmente esistono in capo al fornitore di servizi di comunicazione elettronica accessibili al pubblico, obblighi informativi per lo più preventivi (verso gli utenti e verso le autorità di regolazione) relativamente a possibili rischi di violazione. La Direttiva, invece, introduce (i) l'obbligo di notificare *"senza indebiti ritardi"* i casi di violazione di dati personali all'autorità nazionale competente e (ii) l'obbligo di notificare i casi di violazione di dati personali "*all'abbonato o ad altra persona interessata*" quando detta violazione rischia di pregiudicare i dati personali o la vita privata di un abbonato odi altra persona[9]. La comunicazione all'abbonato o ad altra

[8] Analoga informativa deve essere resa al Garante per la privacy e all'Autorità per le garanzie nelle comunicazioni.

[9] Si considera che una violazione pregiudica i dati o la vita privata di un abbonato o di una persona quando implica, ad esempio, "*il furto o l'usurpazione d'identità, il danno fisico, l'umiliazione grave o il danno alla reputazione in relazione con la fornitura di servizi di comunicazione accessibili al pubblico nella Comunità*" (cfr. Considerando n. 61 della Direttiva). Non è invece richiesta la notifica di una

persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione all'autorità nazionale competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio. I fornitori devono inoltre predisporre e mantenere un inventario delle violazioni dei dati personali (che contiene unicamente le informazioni necessarie a tal fine), ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in misura sufficiente per consentire alle autorità nazionali competenti di verificare il rispetto degli obblighi sopra menzionati. È Infine prevista una sorta di esecuzione forzosa di tali obblighi: infatti, se il fornitore di servizi non ha provveduto a notificare all'abbonato o all'interessato la violazione dei dati personali nei casi previsti, l'autorità nazionale competente, considerate le presumibili ripercussioni negative della violazione, può obbligare il fornitore in questione a farlo. Il potere delle autorità nazionali competenti in materia si estende anche alla emanazione di orientamenti e istruzioni relative alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione. Tali autorità possono infine verificare se i fornitori hanno adempiuto ai loro obblighi di comunicazione e irrogano sanzioni appropriate in caso di omissione.

3.2. Le informazioni raccolte nei riguardi dell'abbonato o dell'utente.

La Direttiva introduce rilevanti modifiche anche per quanto riguarda "*l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un*

---

violazione dei dati personali a un abbonato o a una persona interessata se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

abbonato o di un utente". Si tratta in sostanza dei software che registrano le azioni dell'utente in modo surrettizio e/o pregiudicano il funzionamento dell'apparecchiatura terminale di un utente («software spia» o «spyware») scaricati inconsapevolmente dalle reti di comunicazione elettronica o installati in modo surrettizio nei software distribuiti su supporti esterni per la memorizzazione dei dati quali CD, CD-ROM o chiavi USB. I tentativi da parte di terzi di archiviare le informazioni sull'apparecchiatura di un utente o di ottenere l'accesso a informazioni già archiviate possono perseguire una varietà di scopi che possono essere legittimi (ad esempio alcuni tipi di marcatori, «cookies») o implicare un'intrusione ingiustificata nella sfera privata (come detto, i software spia o virus). Sul punto, la direttiva 2002/58 prevedeva l'obbligo del fornitore di informare in modo chiaro e completo l'utente o l'abbonato circa gli scopi del trattamento. Detto trattamento era consentito laddove fosse offerta all'utente o all'abbonato *"la possibilità di rifiutare tale trattamento*". Ora la Direttiva prevede che "*l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso*[10]*, dopo essere stato informato in modo chiaro e completo*" chiarendo e rafforzando dunque il meccanismo cosiddetto dell'*opt-in*[11]. Resta salvo il diritto per i fornitori di procedere a tali trattamenti per l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

Nella direzione del rafforzamento di meccanismi di consenso preventivo va anche la modifica introdotta dalla Direttiva circa l'utilizzo dei dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica a fini della commercializzazione dei servizi di comunicazione elettronica o per la

[10] Il Considerando 66 della Direttiva chiarisce che il consenso dell'utente al trattamento può essere espresso mediante l'uso delle opportune impostazioni di un motore di ricerca o di un'altra applicazione, qualora ciò si riveli tecnicamente fattibile ed efficace.

[11] Nel Codice della privacy, l'obbligatorio consenso preventivo è tra l'altro già richiesto dall'art. 122.

fornitura di servizi a valore aggiunto. Se la direttiva 2002/58 prevedeva la facoltà per il fornitore di sottoporre a trattamento tali dati per la commercializzazione purchè l'abbonato o l'utente a cui i dati si riferiscono "*abbia dato il proprio consenso*", ora la Direttiva chiarisce detto consenso deve essere "*espresso preliminarmente*" (e – come già sotto il vigore della direttiva del 2002 - il consenso al trattamento dei dati relativi al traffico per le finalità menzionate può essere revocato in qualsiasi momento).

3.3. Le modifiche alla disciplina sulle comunicazioni indesiderate.

Meritano opportuni approfondimenti le modifiche che la Direttiva ha introdotto in materia di comunicazioni indesiderate, già disciplinate dall'art. 13 della direttiva 2002/58 che ora è integralmente sostituito dalle disposizioni che di seguito si esaminano. Una prima modifica ha riguardato l'estensione dell'obbligo del consenso preventivo da parte degli abbonati o utenti rispetto a trattamenti a fini di commercializzazione diretta svolti mediante l'uso di "*sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica*". Tale consenso preliminare va ora richiesto non solo in caso di uso di "sistemi automatizzati di chiamata" ma anche in caso di uso di qualsiasi "sistema automatizzato di comunicazione"[12].

Un altro rafforzamento delle norme contro il fenomeno cosiddetto dello "*spamming*" è contenuto nella nuova norma della Direttiva che si ricollega anche alla direttiva comunitaria 2000/31/CE sui Servizi della Società dell'Informazione (anche nota come Direttiva sul commercio elettronico). La Direttiva, nel confermare quanto già previsto dal previgente testo del 2002, e cioè che è vietata la prassi di inviare

[12] Si noti come il Codice della privacy già preveda tale obbligo all'articolo 130, comma 2: "L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo".

messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni, aggiunge ulteriori divieti. Il primo riguarda la proibizione di inviare messaggi di posta elettronica a scopi di commercializzazione diretta "*in violazione dell'articolo 6 della Direttiva 2000/31/CE*" (che disciplina le comunicazioni commerciali)[13]. Il secondo divieto è quello di esortare i destinatari di messaggi di posta elettronica a scopi di commercializzazione diretta "*a visitare siti web che violino il predetto articolo*". Si vieta cioè ogni forma di pubblicità degli *spammers*.

Ma sicuramente la modifica più interessante in materia di comunicazioni commerciali indesiderate riguarda il nuovo potere di denuncia degli *spammers* ora codificato dal nuovo comma 6 introdotto dalla Direttiva all'art. 13 della direttiva 2002/58/CE. E' infatti previsto che in sede di recepimento gli Stati Membri dovranno garantire che ogni persona fisica o giuridica che abbia subito effetti pregiudizievoli a seguito delle violazioni delle disposizioni in materia di comunicazioni commerciali indesiderate e che abbia un interesse

[13] Cfr. art. 6 (*Informazioni da fornire)*: "Oltre agli altri obblighi di informazione posti dal diritto comunitario, gli Stati membri provvedono affinché le comunicazioni commerciali che costituiscono un servizio della società dell'informazione o ne sono parte integrante rispettino le seguenti condizioni minime:
a) la comunicazione commerciale è chiaramente identificabile come tale;
b) la persona fisica o giuridica per conto della quale viene effettuata la comunicazione commerciale è chiaramente identificabile;
c) le offerte promozionali, come ribassi, premi od omaggi, qualora permesse dallo Stato membro in cui è stabilito il prestatore, devono essere chiaramente identificabili come tali; le condizioni per beneficiarne devono essere facilmente accessibili e presentata in modo chiaro e inequivocabile;
d) i concorsi o giochi promozionali, qualora siano permessi dallo Stato membro in cui è stabilito il prestatore, devono essere chiaramente identificabili come tali; le condizioni di partecipazione devono essere facilmente accessibili e presentate in modo chiaro ed inequivocabile".
Si noti che tale disposizione è stata recepita in Italia nell'art. 8 (rubricato "*Obblighi di informazione per la comunicazione commerciale*") del decreto legislativo 9 aprile 2003, n. 70 di implementazione della direttiva 2000/31/CE.

legittimo alla cessazione o al divieto di tali violazioni, in particolare un fornitore di servizi di comunicazione elettronica che intenda tutelare i propri legittimi interessi commerciali, abbia il diritto di promuovere un'azione giudiziaria contro tali violazioni. Come si intuisce, tale nuova disposizione tutela non solo la riservatezza, ma lo svolgimento corretto di dinamiche competitive nel mercato, evitando che siano sfavoriti – rispetto agli *spammers* - gli operatori che invece trattano correttamente i dati in conformità al quadro normativo in materia di comunicazioni commerciali.

Altrettanto rilevante, infine, è la disposizione (sempre contenuta nel nuovo comma 6 dell'art. 13) in base alla quale gli Stati membri possono inoltre stabilire regole specifiche relative alle sanzioni applicabili ai fornitori di servizi di comunicazione elettronica che "*con la loro negligenza*" contribuiscono alla violazione delle disposizioni in materia di comunicazioni commerciali indesiderate (viene punito cioè una sorta di "spamming preterintenzionale" ….).

3.4. Conclusioni: rinvio alle modifiche dell'impianto sanzionatorio.

Infine, va segnalato che la Direttiva incide anche sugli aspetti sanzionatori per i casi di violazione delle norme. Il nuovo articolo 15-*bis* della direttiva 2002/58/CE prevede infatti che gli Stati Membri dovranno determinare specifiche sanzioni, "*incluse, se del caso, sanzioni penali"* , da irrogare in caso di violazione delle norme nazionali di attuazione. Le sanzioni previste dovranno essere "*effettive, proporzionate e dissuasive*" e potranno essere applicate per coprire la durata della violazione, e addirittura "*anche se a tale violazione è stato successivamente posto rimedio*". Se si considera – ad esempio – l'impianto sanzionatorio del Codice della privacy, che tra l'altro è stato fortemente inasprito con un intervento legislativo del 2008, ci si deve attendere – in sede di implementazione della Direttiva – un ulteriore aggravamento delle sanzioni ("*incluse, se del caso, sanzioni penali"*).

Tecnologie DRM e TPM per la protezione delle opere e implicazioni sulla privacy degli utenti finali

di Elena Finotti [*]

SOMMARIO: 1. Premessa – 2. Cosa proteggono i sistemi DRM e TPM – 3. Chi ci protegge da DRM e TPM? – 4. I rischi e l'ammissibilità della profilazione degli utenti. – 5. Conclusioni

1. Premessa.

Da un punto di vista tecnico, quando si parla di DRM e di TPM si entra nel mondo dell'informatica al servizio della sicurezza e della proprietà. Questi due elementi, infatti, sono principalmente utilizzati per determinare e circoscrivere la fruizione di beni e servizi digitali, commercializzati *on-line* o su supporti fisici, che assolvendo alla protezione di interessi tutelati dall'ordinamento, sono da lungo tempo riconosciuti a livello internazionale[1] e nazionale. L'uso di DRM e TPM è stato ed è tutt'ora, al centro di aperte discussioni e vivaci dibattiti, tra fautori e detrattori, soprattutto per le difficoltà di

[*] Avvocato civilista in Latina, specializzata in Diritto delle nuove tecnologie; Istituto Italiano per la Privacy.

[1] I principali riferimenti Internazionali sono: La convenzione di Berna (Berne Convention for the Protection of Literary and Artistic Works) al link: http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html; Il trattato TRIPs del 1994 (Agreement on Trade Related Aspects of Intellectual Property Rights) al link http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm; Il WIPO Copyrights Treaty del 20 dicembre 1996, consultabile all'indirizzo: http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html; il WIPO Performances and Phonograms Treaty del 23 dicembre 1996, al link: http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html#P98_10339.
L'implementazione statunitense di questi trattati è stata operata con il DMCA (Digital millenium copyright act) del 1998, al link www.copyright.gov/legislation/dmca.pdf; mentre il recepimento europeo è avvenuto con la Direttiva 29/2001/CE citata successivamente.

conciliare la tutela della proprietà intellettuale (cui questi strumenti sono principalmente destinati) con la libertà e la riservatezza degli utenti. Tutti i diritti in gioco, infatti, sono considerati rilevanti per l'ordinamento e la prevalenza dell'uno sull'altro non è affatto scontata. La difficoltà di stabilire a quale spetti la preponderanza è data dalla complessità delle modalità tecnologiche attraverso cui passano e si concretizzano questi diritti. Per entrambi abbiamo la stratificazione di un interesse individuale con uno collettivo.

Da una parte i possessori del contenuto dell'opera (c.d. content holders), che sono titolari di un interesse personale allo sfruttamento ma anche di un interesse collettivo di tipo economico: senza la remunerazione della commercializzazione, i principi di mercato ne verrebbero stravolti con conseguente perdita di interesse nelle attività di finanziamento di nuove idee. La digitalizzazione delle opere ne garantisce maggiore qualità e diffusione ma le espone al rischio di una diffusione abusiva e selvaggia. D'altro canto però, ogni utente/consumatore ha il diritto di fruire dell'opera (diritto acquistato, peraltro, solitamente, a titolo oneroso) senza essere trasformato in una variabile economica variamente sfruttabile, né a livello collettivo è immaginabile l'accettazione di una lesione macroscopica della privacy in funzione di interessi, comunque, soggettivi e privati. L'identità digitale degli utenti è ormai equiparabile a quella reale e deve essere fortemente difesa da qualsiasi ingerenza esterna. Il conflitto c'è e non è di poco conto.

2. Cosa proteggono i sistemi DRM e TPM

Con l'acronimo DRM (Digital Rights Management, letteralmente "Gestione dei diritti digitali") si indica la disciplina tecnologico-giuridica che serve a determinare la fruizione dei diritti di proprietà intellettuale. I sistemi di management digitale vengono utilizzati per gestire e proteggere il contenuto delle opere digitalizzate e possono, pertanto, riguardare sia i supporti fisici su cui è immagazzinato il contenuto digitale (ad esempio CD o DVD), sia i formati *on line* destinati all'e-commerce (ad esempio e-book, file musicali, *video on demand* etc.). Attraverso il DRM si ottiene quindi, sia il

riconoscimento del bene come "autentico", sia la determinazione di cosa si possa fare con quel bene. La prima funzione (quella di riconoscimento) viene ottenuta attraverso l'applicazione di marchi, fisici o virtuali (ne sono esplicazione tanto il bollino SIAE quanto il watermark[2]). La seconda funzione – la disciplina d'uso – viene invece determinata da licenze di commercializzazione e da funzionalità tecnico-informatiche inserite nel prodotto/servizio. L'uso del DRM soddisfa quindi l'esigenza di protezione delle opere sotto due profili. Uno è quello oggettivo: rispetto alla fruizione con modalità non autorizzate; è il caso, ad esempio della limitazione definitiva e congenita all'uso del prodotto ottenuta con l'inserimento di sistemi di blocco di alcune funzionalità, spesso "nascosti" all'interno del prodotto digitale. L'altro è quello soggettivo: rispetto alla fruizione da parte di soggetti non legittimati. E' quanto avviene attraverso l'inserimento di un meccanismo di riconoscimento e attivazione che consente lo sblocco del contenuto tramite la chiave di decodificazione[3] attribuita solo ad utente registrato o riconosciuto.

La gestione e la portata delle limitazioni inserite dai DRM sono conoscibili per l'utente/acquirente solo tramite licenza d'accesso fornita, quasi sempre, separatamente rispetto al prodotto acquistato. La modalità di accettazione e di sottoscrizione di tali licenze contiene tutte le problematiche poste dalla disciplina dei contratti digitali[4]. Il più delle volte, infatti, tali licenze vengono "accettate" tramite

[2] Il Watermark è una sorta di "bollino" o traccia digitale inserita all'interno di immagini, testi, canzoni e quant'altro, con il fine di permettere di verificare se un esemplare è stato autorizzato oppure no e garantirne l'originalità. Assolve, quindi, alla funzione di marchio di proprietà e certificato di autenticità digitale.

[3] Un esempio pratico: Microsoft è stata la prima azienda a caricare un meccanismo DRM di attivazione dei software sui suoi prodotti. Con il programma "Microsoft Reader", destinato alla lettura degli e-book, i prodotti acquistati venivano protetti dal rischio di copiatura mediante un sistema di riconoscimento on-line. In pratica l'utente veniva connesso automaticamente ad un server incaricato di controllare il dispositivo ed il file. Se le informazioni decodificate dal server corrispondevano ad un prodotto "autentico", il sistema veniva sbloccato. La procedura è stata ormai implementata in tutti i successivi prodotti Microsoft.

[4] Per una panoramica completa sull'argomento vedi E. TOSI, *Il Contratto Virtuale. Procedimenti formativi e forme negoziali tra tipicità e atipicità*, Milano, Giuffrè, 2005

l'apertura della confezione di un CD/DVD o cliccando direttamente sul download di file dal web.

La sigla TPM indica il sistema Trusted Platform Module (traducibile letteralmente come "Modulo di piattaforma affidabile o fidata"). Come nel caso del DRM, l'acronimo viene utilizzato per indicare sia le regole che gli strumenti di applicazione da esse generati. Nel caso dei TPM[5] l'abbreviazione indica sia le modalità tecniche di costruzione di una piattaforma di sicurezza informatica, sia il chip prodotto in base alle stesse. Il funzionamento del TPM è legato ad una combinazione crittografia: ogni chip è dotato di una coppia univoca di chiavi crittografiche e di un motore di crittografia asimmetrica per la crittazione dei dati che in abbinamento a specifici software consentono il controllo di alcune operazioni. Di fatto il controllo di sicurezza operato tramite TPM avviene sotto forma di registrazione delle operazioni compiute dall'utente, in appositi registri interni detti PCR (Platform Configuration Register), che registrano lo stato del sistema raffrontando il prima e il dopo delle operazioni compiute. L'uso primario di tali sistemi, che possono essere presenti su qualsiasi strumento o piattaforma, è quella di inibire determinati comandi, sia in funzione di salvaguardia (ad esempio, bloccare la connessione a una rete considerata non affidabile) sia con funzione di controllo (ad esempio impedendo l'istallazione di un software non autentico). Le notazioni tecniche riportate farebbero ritenere che gli unici profili di rilevanza normativa di tali dispositivi dovrebbero essere legati alla gestione dei rapporti commerciali con gli utenti fruitori delle opere. Questi, infatti, sono indotti all'accettazione delle limitazioni dei diritti di godimento e d'uso, (limitazioni di cui ignorano perlopiù il contenuto e la portata)[6] in quanto condizionati da

[5] Il chip TPM è noto anche come "Chip Fritz", in onore del Senatore Statunitense Ernest "Fritz" Hollings, che si è distinto per l'appoggio politico dato alla legalizzazione d'uso di questi strumenti.

[6] E' molto rilevante in tal senso la *querelle* giuridica sul diritto di copia privata, riconosciuta al fruitore dell'opera dall'art. 71 sexies comma 4, L. 633/1941, diritto che viene automaticamente annullato dall'implementazione dei sistemi di protezione citati, che impediscono, di fatto, di effettuare copie. La giurisprudenza italiana è prevalentemente orientata a legittimare la compressione del diritto individuale a favore della tutela del diritto d'autore. Vedi *ex multis* Tribunale di Milano, 1 luglio

un'abissale difformità di libertà contrattuale con i fornitori dei beni e dei servizi. In realtà tali strumenti presentano elementi di problematicità anche in relazione alla raccolta occulta di dati personali.

3. Chi ci protegge da DRM e TPM?

L'uso dei DRM e dei TPM ha trovato iniziale accoglimento in ambito comunitario con l'approvazione della Direttiva 2001/29/CE[7] art. 47, che ha legittimato l'uso delle protezioni tecnologiche, invitando contestualmente gli stati membri "*Per evitare soluzioni legislative frammentarie che potrebbero ostacolare il funzionamento del mercato interno"* a "*prevedere una protezione giuridica armonizzata contro l'elusione di efficaci misure tecnologiche"* [8] . Frutto del recepimento di tale Direttiva, è l'attuale formulazione dell'art.102 quater, comma 1 della L. 633/1941 in materia di Diritto d'Autore: "*I titolari di diritti d'autore e di diritti connessi nonché del diritto di cui all'art. 102-bis, comma 3, possono apporre sulle opere o sui materiali protetti misure tecnologiche di protezione efficaci che comprendono tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o*

2009 in "Diritto dell'Informazione e dell'Informatica", n. 4/5 2009, pag. 763 e ss.; anche in Europa la tendenza è ampiamente affermata, vedi ad esempio la famosa Sentenza n. 549 del 28 febbraio 2006 della I° sez. civ. della Corte di Cassazione francese, nella quale si è stabilito che il diritto alla copia privata non può limitare l'uso dei Drm da parte dei produttori, per un commento e un raffronto della Sentenza con l'ordinamento italiano vedi: A. MONTI "DRM: in Italia la copia privata è un diritto", al link http://www.interlex.it/copyright/amonti85.htm.

[7] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione. Consultabile integralmente in lingua italiana al link: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:IT:PDF.

[8] Per un commento specifico sul punto v. L. CHIMIENTI, *La nuova proprietà intellettuale nella Società dell'informazione*, Milano, Giuffrè, 2005, pag. 81 e ss.

limitare atti non autorizzati dai titolari dei diritti." [9]. Gli aspetti presi in considerazione dalla normativa, sono, quindi, esclusivamente volti alla considerazione dell'efficacia deterrente degli strumenti rispetto alla violazione dei diritti d'autore, problematica sicuramente molto rilevante, ma non l'unica da valutare. Infatti, mentre costituiscono una barriera per i "pirati" e un valido mezzo di gestione personalizzata dei servizi offerti (perché possono consentire una differenziazione e una flessibilità personalizzata d'accesso), DRM e TPM sono contemporaneamente potenti strumenti di raccolta di dati personali. Ci sono, infatti, degli aspetti complessi che coinvolgono la raccolta di dati personali e che interessano soprattutto i servizi on-line. Ciò può avvenire con due modalità,

- in modo diretto, per la natura e il funzionamento proprio di queste tecnologie;
- in modo indiretto, attraverso strumenti "agganciati" a tale tecnologie, che possono essere sfruttabili per la raccolta dei dati.

Con riferimento alla raccolta diretta, la funzione di gestione dei servizi, implica in sé una raccolta di dati personali: nominativo, indirizzo, numero della carta di credito dell'utente. Tali dati, in quanto qualificabili come "dati personali" dal Codice della privacy (D.Lgs 196/2003), sono pacificamente inseriti nel contesto di protezione generale costruito in termini di informativa, consenso, autorizzazione al trattamento. Ma non sono gli unici dati che vengono raccolti dai sistemi di gestione DRM e TPM, questi, infatti, memorizzano "naturalmente" anche informazioni relative a: cosa ha scelto un determinato utente, quando il prodotto è stato acquistato, quando e come ci si è collegati al server del fornitore per fruire del servizio *on demand*, che tipo di tecnologia il consumatore ha a disposizione per accedere al prodotto (software e hardware del pc, dello smartphone o di ogni altro strumento di connessione). Questi dati, che possono

[9] Il successivo comma 2 definisce invece i parametri di riferimento per l'efficacia delle protezioni tecnologiche: "*Le misure tecnologiche di protezione sono considerate efficaci nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o del materiale protetto, ovvero sia limitato mediante un meccanismo di controllo delle copie che realizzi l'obiettivo di protezione*".

essere molto rilevanti a fini di marketing o di pubblicità, costituiscono la base per una successiva attività di profilazione, cioè per la creazione di una entità commerciale ritagliata, attraverso il c.d. *data mining*[10], sull'analisi dei comportamenti del consumatore/utente. Tramite le profilazione, inoltre, il gestore del servizio potrebbe acquisire indirettamente dati di natura sensibile aggirando gli obblighi specifici previsti dalla normativa in materia. Se, ad esempio, dall'analisi statistica del comportamento dovesse rilevarsi la ricorrenza di una determinata informazione (quale potrebbe essere l'acquisto di materiale caratterizzante una determinata tendenza sessuale) ciò potrebbe comportare l'acquisizione illecita di una informazione sensibile.

La seconda ipotesi, quella di una raccolta "indiretta" di dati è legata invece al collegamento dei sistemi DRM con altri strumenti informatici con funzionalità diverse, solo indirettamente collegate alla tutela del diritto d'autore. In questo caso, oltre alle problematiche intrinsecamente esistenti sulle tecnologie DRM e TPM possono aggiungersene altre relative agli strumenti ad essi agganciati. Un esempio pratico può chiarire meglio il concetto. Questo tipo di tecnologia "ibrida" è balzato agli onori della cronaca, con lo scandalo "Sony rootkit", La nota casa discografica aveva commercializzato CD musicali protetti dal sistema DRM XCP. Tale tecnologia comporta l'installazione sul sistema "ospite" dell'utente, di un sistema di rootkit, con la funzione di evitare l'aggiramento dei meccanismi di protezione DRM. Il rootkit, installato inconsapevolmente dall'utente, costituisce una sorta di "porta segreta" al sistema che può essere utilizzata dai malintenzionati per inserire del malware (trojan, virus, worm) difficile da rimuovere con i normali antivirus proprio perché posizionato in una zona d'invisibilità non rilevata. In questi casi le problematiche relative alla privacy, pur essendo di natura eventuale, sono molto ampie e tangenti la perdita generale di sicurezza del sistema utilizzato (pc, smartphone o qualsiasi altra piattaforma), il

[10] È l'esame complessivo dei dati raccolti sull'attività dei propri utenti/clienti, tendente a trovare nei loro comportamenti correlazioni significative da un punto di vista commerciale.

fenomeno quindi, meriterebbe un'analisi ben più approfondita di quella possibile in questa sede.

4. I rischi e l'ammissibilità della profilazione degli utenti.

Torniamo quindi alla raccolta di dati effettuata direttamente tramite DRM e TPM. La delicatezza della questione ha indotto il Garante a pronunciarsi in materia di profilazione[11], fornendo una serie di prescrizioni ai fornitori di servizi di comunicazione elettronica, dove per servizi di comunicazione elettronica devono intendersi quelli consistenti esclusivamente o prevalentemente "nella trasmissione di segnali su reti di comunicazioni elettroniche" (ex art. 4, comma 2, lett. d) ed e) del Codice privacy). Vi rientrano quindi, pacificamente, anche i fornitori di servizi che utilizzano i sistemi DRM e TPM, nei casi in cui la fruizione da parte degli utenti avvenga on-line. In realtà le regole generali poste dal Garante, in quanto basate sui principi generali della normativa privacy costituiscono un valido punto di riferimento per la profilazione comunque intesa ed operata. Secondo quanto stabilito nel Provvedimento citato, l'attività di profilazione può avere ad oggetto tre tipologie di dati: dati anonimi, dati personali individuali, dati personali "aggregati".

I dati anonimi[12] sono gli unici che non comportano alcun problema poichè vengono raccolti in modo impersonale e scollegato da riferimenti individuali. L'analisi del comportamento avviene quindi su di un'utenza media e con valutazioni generalizzate.

I dati personali individuali sono quelli raccolti separatamente dal fornitore del servizio e sono sempre riferibili ad un utente determinato. In questo caso l'attività di profilazione sarà consentita con il rispetto di alcune prescrizioni. In particolare, il fornitore del servizio quale titolare del trattamento di raccolta e analisi dei dati sarà tenuto: i) a rendere agli interessati l'informativa specifica in relazione

[11] Cfr. Garante per la protezione dei dati personali, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione*, in G.U. n. 159 dell'11 luglio 2009.

[12] I dati che siano qualificabili come anonimi ai sensi dell'art. 4, c. 1 lett. n) del Codice privacy.

alle finalità perseguite con l'attività di profilazione e ai diritti esercitabili dall'utente ai sensi dell'art. 7 del Codice (art. 13 del Codice privacy); ii) a documentare per iscritto il consenso informato, libero e specifico manifestato dall'interessato per le attività di profilazione (art. 23 del Codice privacy); iii) c) a notificare al Garante il trattamento dei dati a fini di profilazione (art. 37 comma 1, lett. d) del Codice privacy) [13].

I dati personali aggregati sono tutti i dati raccolti dal fornitore del servizio, afferenti all'individuazione del soggetto o alle attività da questo svolte in relazione al servizio prestato, non considerati singolarmente ma aggregati tra loro. Tali dati vengono utilizzati e analizzati secondo regole di valutazione diverse da titolare a titolare. In relazione alla profilazione aggregata, il fornitore potrà pacificamente svolgere la propria attività ove abbia provveduto a rendere agli interessati l'informativa specifica in relazione alle finalità perseguite e ai diritti esercitabili dall'utente ed a notificare al Garante il trattamento dei dati a fini di profilazione.

Diversamente si pone invece la questione del consenso. Il fornitore del servizio potrà raccogliere il consenso informato, libero e specifico per l'attività di profilazione aggregata, oppure, in assenza di questo, procedere a richiedere una verifica preliminare del trattamento al Garante (mediante la procedura prevista dall'art. 17 del Codice privacy), per verificare se tale trattamento sia lesivo dei diritti personali riconosciuti dall'ordinamento. Il Garante procederà quindi ad una valutazione "*in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che il trattamento può determinare. Solo in quella sede, infatti, sarà possibile valutare, tra le altre condizioni, se sia possibile autorizzare il trattamento avente ad oggetto tali dati, anche in assenza del consenso degli interessati, ai sensi dell'art. 24, comma 1 lett. g) del Codice*"[14], e fornirà le indicazioni necessarie per

[13] Art. 37 comma 1: Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda: […] lett. d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

[14] Provv. citato

l'eventuale adeguamento alla normativa. E' ammissibile, quindi, un trattamento di profilazione senza espressione di consenso da parte degli interessati, purché autorizzato esplicitamente dal Garante. La profilazione aggregata viene così ricondotta all'istituto del *prior checking*, ad una valutazione prodromica riservata ai trattamenti che presentano rischi specifici per l'interessato. Riassumendo, il fornitore che intenda lecitamente operare attività di profilazione aggregata dovrà: a) rendere agli interessati l'informativa specifica in relazione alle finalità perseguite con l'attività di profilazione e ai diritti esercitabili dall'utente ai sensi dell'art. 7 del Codice (art. 13 del Codice privacy); b) documentare per iscritto il consenso informato, libero e specifico manifestato dall'interessato per le attività di profilazione aggregata (art. 23 del Codice privacy) o, in alternativa, richiedere una verifica preliminare del trattamento al Garante ai sensi dell'art. 17 del Codice privacy, adeguandosi alle prescrizioni ricevute; c) notificare al Garante il trattamento dei dati a fini di profilazione aggregata (art. 37 comma 1, lett. d) del Codice privacy).

5. Conclusioni.

La profilazione aggregata è certamente quella più interessata dall'uso degli strumenti DRM e TPM, che proprio per l'intrinseca natura di elementi di gestione dei servizi offerti raccolgono una mole di dati di natura diversa (identificativi, sui tempi di connessione, sulle modalità di pagamento etc. etc.). Questa mole di dati costituisce un *asset* significativo per le società dal punto dell'analisi commerciale e del marketing personalizzato. Quindi escludendo l'ipotesi residuale di un'anonimizzazione successiva alla raccolta, di fatto DRM e TPM costituiscono dei collettori importantissimi di dati personali. In relazione a ciò gli unici elementi di tutela sono: la prestazione del consenso su informativa e il controllo preventivo del Garante privacy in assenza del controllo stesso. *Nulla quaestio* sulla seconda ipotesi: il controllo del Garante è sicuramente idoneo a verificare la correttezza del procedimento. Per quanto riguarda il consenso informato, invece, sorge qualche dubbio sull'effettiva capacità dell'utente di percepire e comprendere la natura del trattamento dei dati raccolti tramite DRM e

TPM. Se, infatti, l'utente è consapevole di fornire i propri dati identificativi per l'accesso al servizio, non è altrettanto scontato che lo sia di essere "registrato" in ogni sua singola operazione di fruizione del servizio, né che tali registrazioni possano generare la costruzione di un profilo commerciale a lui riferibile. In questo caso l'informativa dovrebbe essere veramente molto chiara, non limitandosi a fare riferimento ad una generica modalità di aggregazione dei dati ma esplicitando i criteri di ogni singola operazione.

La prestazione di un valido consenso informato, inoltre dovrebbe essere subordinata alla consapevolezza che il prodotto/servizio scelto e fruito contiene un sistema di gestione DRM o TPM. Infatti, mentre è disciplinato l'uso di tali tecnologie, manca, sia a livello comunitario che nazionale, un regolamento per i contrassegni da apporre sulle opere protette da tali sistemi. Tali contrassegni potrebbero essere differenziati, ad esempio, in relazione a tabelle relative alla tipologia di limitazioni sul bene (diritto di copia, fruizione entro un lasso temporale determinato, fruizione limitata a un certo numero di volte etc.) e alla natura anonima o personale dei dati raccolti. Sicuramente si determinerebbe un sistema complesso, ma di maggior trasparenza per l'utente finale che potrebbe percepire immediatamente (e scegliere correttamente) la tipologia di prodotto o servizio.

Attualmente, infatti, l'indicazione della presenza di DRM e TPM viene rimessa all'iniziativa individuale dei fornitori che in assenza di una consapevolezza specifica da parte degli utenti e di una relativa ricaduta sulla propria immagine societaria, non hanno interesse a pubblicizzare chiaramente l'uso di tali tecnologie. Infatti, escludendo i casi particolari in cui l'esistenza della tecnologia è stata "scoperta" dagli utenti, (come nello scandalo "Sony - rootkit" citato sopra) manca una chiara esplicazione delle modalità di business scelte dalle aziende, che sembrano più concentrate alla lotta alla pirateria che alla creazione di un sodalizio commerciale con gli utenti "onesti".

Si auspica quindi l'apertura di un ampio dibattito sul punto che potrebbe portare all'adozione di soluzioni condivise di tutela della privacy dei consumatori/utenti senza pregiudicare gli interessi dei fornitori all'uso di tali tecnologie.

La privacy sta cambiando ?
Dalle privacy-enhancing technologies (PETs) alla privacy by design (PbD)

di Nicola Fabiano [*]

SOMMARIO: 1. Introduzione. – 2. La rete Internet, le risorse e i dati personali. – 3. La cultura della privacy e le nuove tecnologie. – 4. Privacy e futuro: *Internet of Things*. – 5. Tutela dei dati personali e profili tecnologici: dalle PETs alla Privacy by design. – 6. Conclusioni.

1. Introduzione.

L'evoluzione tecnologica, nel corso degli ultimi tempi, ha inciso sulle modalità di comunicazione, tanto da influenzare addirittura la nostra vita quotidiana. In effetti, è semplice osservare come siano modificate le abitudini della vita privata e di quella lavorativa: si avverte una sempre maggiore esigenza di comunicare attraverso la rete Internet e le risorse ad essa connesse. Tale mutamento ha avuto un'incidenza così profonda che a volte la comunicazione e l'utilizzo delle risorse tecnologiche più recenti diviene prioritaria rispetto ad altri aspetti come, ad esempio, quello della tutela dei dati personali. Non c'è da meravigliarsi se si preferisce utilizzare immediatamente una determinata risorsa disponibile in rete piuttosto che riflettere preventivamente sulla sorte dei propri dati personali; a ciò si aggiunga la scarsa attenzione degli utenti riguardo alle informative e alle privacy policy che sono pubblicate (ma non sempre è così) su Internet.

Pertanto, al di la degli aspetti di natura propriamente sociologica che esulano dal presente contributo, è interessante soffermarsi sulle modalità di tutela dei dati personali in Internet e sulle risorse

[*] Avvocato, patrocinante in Cassazione, Specialista in Diritto Civile; Istituto Italiano per la Privacy.

tecnologiche eventualmente idonee a contribuire alla protezione delle informazioni degli utenti.

2. La rete Internet, le risorse e i dati personali.

La rete Internet, per sua natura, si presta ad essere facilmente identificata come 'pericolosa' per i dati personali. Un simile approccio è certamente scorretto, posto che non va condannata aprioristicamente Internet, che – al contrario – è una risorsa preziosa per l'intera umanità; piuttosto, è necessario che si analizzi, dall'altro lato, il comportamento dell'utente. Un dato è certo e scontato: non si può imputare alla rete Internet la diffusione e la divulgazione dei dati personali di un soggetto, poiché necessariamente essi saranno stati canalizzati da qualcuno. Le numerosissime risorse presenti sulla rete Internet (social network, forum, chat, siti web, ecc.) dovrebbero essere regolamentate da quelle che si definiscono privacy policy, ossia una sorta di regolamento che disciplini le modalità con cui i dati personali vengono trattati. Ipotizzando che tali risorse ne siano adeguatamente dotate nel rispetto della normativa (l'individuazione delle norme dipende dal luogo in cui vengono trattati i dati), molto spesso gli utenti non realizzano perfettamente le modalità di queste policy e frequentemente saltano "a pie' pari" la lettura dell'informativa che viene loro sottoposta (magari spuntando la voce "accetto" o similare). D'altro canto, sul fronte degli utenti, potrebbero esserci delle persone che non hanno particolare dimestichezza con la normativa in materia di privacy e con gli adempimenti ad essa connessi e quindi, anche se "*ignorantia legis non excusat*", bypassano (negligentemente) le informazioni circa il trattamento dei dati personali. In questo scenario si collocano le questioni relative ai dati personali e quelle connesse che riguardano l'anonimato, la eID, il diritto alla cancellazione dei propri dati personali in un contesto qual è quello di Internet. Con riferimento all'anonimato, autorevole dottrina[1] che più recentemente

[1] Cfr. G. FINOCCHIARO, voce Anonimato in *Digesto delle discipline privatistiche*, Iannarelli-Rook Basile-Sacco-Scala (con la collaborazione di), Sez. civ., Agg., Torino, 2010.

si è occupata *ex professo* dell'argomento anche con riguardo ai profili della rete Internet preliminarmente rileva come la definizione di anonimato va ricercata nella "collegabilità fra le informazioni e il soggetto cui si riferiscono". In buona sostanza, perché vi sia anonimato, deve risultare impossibile l'associazione tra i predetti elementi, ossia delle informazioni da un lato e del soggetto dall'altro. Si tratta, ovviamente di un'analisi che finisce con il postulato della impossibilità di un anonimato assoluto, posto anche che non esiste legislazione che disciplini tale fenomeno. Del resto, la stessa dottrina appena citata afferma l'inesistenza di un diritto o di un dovere all'anonimato. Evidentemente l'attenzione per l'anonimato e l'esigenza da parte di taluni di utilizzare una simile soluzione è spiegabile con l'evoluzione delle tecnologie e con il sempre maggior utilizzo della rete Internet che vede aumentare vorticosamente la propria popolazione. Molto spesso l'anonimato viene avvertita come un'esigenza concreta, soprattutto da parte degli e-cityzen, di precostituirsi una tutela reale nelle vicende (anche negoziali) che li vede presenti sulla rete Internet. Da un lato, quindi, non sussistono risorse normative specifiche sull'anonimato, ma d'altro canto è senz'altro possibile realizzare in concreto l'anonymity attraverso le risorse tecnologiche; è auspicabile – *de iure condendo* – che si possa disciplinare detto fenomeno, anche per attribuire piena attuazione al principio sancito dall'art. 1 del codice privacy (D.Lgs. 196/2003) del "diritto alla protezione dei dati personali" che, diversamente, sotto questo profilo, potrebbe risultare una mera affermazione di principio. Va, comunque evidenziato che, fatte salve le ipotesi in cui la legge impone l'individuazione di un soggetto, argomentando *a contrariis* non sussiste un divieto all'anonimato, proprio quando diventa necessario non vanificare il diritto (perché tale è qualificato) alla protezione dei dati personali. Resta da stabilire con quali modalità tecniche si possa garantire il diritto alla protezione dei dati personali soprattutto nelle ipotesi di navigazione su Internet.

Il concetto di eID, acronimo di electronic Identity, è strettamente connesso a quello di eIDM (acronimo di electronic Identity Management) e sostanzialmente, senza assillare il lettore con troppi tecnicismi, consiste nell'utilizzazione di una o più tecnologie per la gestione della identità digitale anche attraverso il controllo degli

accessi alle risorse. L'argomento eID è utilizzato, oltre che in campo informatico, anche nell'ambito dell'e-Governement; In Italia, difatti, si parla di eID con riferimento alla Carta d'Identità Elettronica (CEI) alla quale sono associati alcuni servizi disponibili per il titolare con il vantaggio di utilizzare un unico dispositivo che sia idoneo ad identificare il soggetto fruitore. Il maggior interesse per la eID, si ribadisce, è nell'ambito dell'e-Governement per l'agevole processo di associazione dei dati del titolare con i servizi pubblici di cui lo stesso può fruire; tuttavia, l'attenzione per la eID è ovviamente anche rivolta per eventuali utilizzi di risorse della rete Internet. In taluni casi sulla rete Internet è molto utile avere la certezza della identità del proprio interlocutore, quanto meno sul piano formale e degli effetti giuridici. Ciò offre una serie di garanzie anche in ordine alla riduzione della rischiosità sui furti d'identità. D'altro canto è pur vero che non sempre può essere utile avere la certezza di essere identificati in rete (il mondo virtuale a volte non presenta situazioni completamente simmetriche a quelle presenti nel mondo reale). Il sistema della eID potrebbe essere utile, però, per la protezione dei dati personali che non saranno intelligibili se non attraverso procedure tecnologiche ed informatiche di autenticazione.

3. La cultura della privacy e le nuove tecnologie.

Discutere di privacy nel corso di questi anni ha sostanzialmente avuto un unico riferimento consistente nel considerare i dati personali quale diritto meritevole di tutela secondo l'ordinamento giuridico. Difatti, il legislatore (quello europeo con la Direttiva 95/46/EC, e quello italiano con il vigente D.Lgs. 196/2003) ha inteso disciplinare il concetto di riservatezza con diretto riferimento ai dati personali. In sostanza il diritto alla riservatezza dei dati personali è stato qualificato come diritto soggettivo e da qui è sorta una vera e propria cultura della privacy fondata unicamente sulla tutela dei dati personali (in Italia il diritto è stato riconosciuto anche alle persone giuridiche che in Europa, invece, non godono di tutela). Il concetto di privacy, pertanto, è stato sempre (o quasi) associato alla tutela riconosciuta dall'ordinamento giuridico ai dati personali in quanto, appunto,

strettamente connessi con la persona. In realtà, siamo stati tutti testimoni di come la privacy abbia rivoluzionato la nostra vita quotidiana, posto che non eravamo assolutamente abituati a convivere con l'idea di salvaguardia delle informazioni personali. Non può sottacersi che nella fase iniziale (ma probabilmente accade ancor'oggi) addirittura la privacy è stata vista come una sorta di ostacolo alle nostre vicende quotidiane; il sentirsi opporre la tutela dei dati personali in determinate circostanze ha irritato non pochi. Tuttavia, si è dovuto convivere con una novità proprio concettuale che andava ad affiancare quelli che sino a pochi anni fa erano i nostri punti fermi tra cui non era presente la privacy.

Attualmente siamo tutti (o dovremmo essere) consapevoli che i dati personali sono meritevoli di tutela secondo l'ordinamento giuridico, ma soprattutto fanno parte del nostro patrimonio culturale. La "presa di coscienza", quindi, della portata culturale, oltre che legale ovviamente, che può essere riconosciuta ai dati personali ha lasciato il campo – soprattutto agli esperti d'oltreoceano – alle teorizzazioni sul concetto di privacy che hanno portato effetti diretti in ambito privacy. Privacy e tutela dei dati personali hanno subito una vera e propria evoluzione nel corso degli anni con gli effetti di un ampliamento concettuale che li porta alla identificazione di profili autonomi ed indipendenti dal dato normativo al quale sono connessi. In sostanza, i dati personali sono rilevanti in quanto tali e non soltanto (o unicamente) perché sono meritevoli di tutela secondo l'ordinamento giuridico. Si propone una lettura dei concetti di privacy e dati personali che prescinde dalla qualificazione degli stessi come diritto (anche fondamentale) perché fanno parte integrante della sfera personale di un soggetto. Non solo ! Secondo questa nuova "lettura" il concetto di privacy assurge ad essere componente essenziale di una società democratica. Da ciò il doppio profilo della privacy sia come elemento di tutela della sfera personale di un soggetto, qualificabile pure come diritto fondamentale, sia come principio democratico. Si tratta, ovviamente, di un approccio evolutivo molto interessante che sicuramente non prescinde dalle tecnologie in generale. Sul fronte delle nuove tecnologie si è dovuto pensare alla tutela dei dati personali. In realtà, come spesso erroneamente si presuppone, non è la tecnologia che determina (anche potenzialmente) la violazione della

privacy, ma è l'uso che se ne fa. La tecnologia è neutra ed assume la colorazione che viene attribuita dall'utente. Pertanto, in un primo momento che risale al 1995 si è iniziato a parlare di Privacy Enhancing Technologies (il cui acronimo è PETs) per fare riferimento a tutti quegli accorgimenti tecnici e tecnologici che possono salvaguardare i dati personali.

Successivamente, l'approccio per così dire "ideale" o concettuale della privacy porta l'Autorità canadese (Information & Privacy Commissioner) ad affrontare la questione della privacy elaborando la teoria della Privacy by Design (il cui acronimo è PbD).

4. Privacy e futuro: *Internet of Things*.

Di recente si sente parlare sempre più spesso di "Internet of Things". Si tratta di uno dei nuovi paradigmi della rete Internet la cui origine si fa risalire al 1998 ad opera di Kevin Ashton. Con l'espressione "Internet of Things" si fa riferimento ad un insieme di oggetti tra loro connessi mediante una specifica tecnologia (la più nota e diffusa è quella RFID, acronimo di Radio Frequency IDentification). Infatti, attraverso la tecnologia RFID più oggetti comunicano tra loro creando una rete di informazioni: si tratta dell'Internet of Things, ossia dell'Internet degli oggetti. Il paradigma dell'Internet of Things (anche noto con l'acronimo IoT) costituisce il profilo più futuristico di Internet, ma preferisco utilizzare un ossimoro per affermare che "l'Internet of Things è il futuro della rete Internet, ossia ciò che viviamo al presente". In effetti, IoT è già il sistema nel quale viviamo in quanto già esistono implementazioni sulla rete di questo nuovo paradigma: si spazia dal sistema di gestione dei magazzini ai servizi fruibili dall'utente (es. l'acquisto di biglietti mediante lo smartphone o il cellulare), agli impianti muniti di sensori controllabili da diverse parti del mondo attraverso la rete. In questo ampio contesto non si possono trascurare gli aspetti del fenomeno che sono connessi con la privacy e con la tutela dei dati personali. In effetti, nell'ipotesi in cui una persona (fisica o giuridica) sia connessa in qualche modo ad uno o più oggetti che, mediante la tecnologia RFID (o anche altra), trasmettano dati sulla rete Internet, sorge la necessità (o meglio

l'obbligo) di trattare i dati personali nel rispetto della normativa. La questione concernente la normativa applicabile diventa più complessa, nell'ipotesi di IoT, poiché, per la natura della stessa rete Internet, potrebbe non è possibile localizzare i dati trattati e quindi determinare esattamente quale norma utilizzare.

Senza volersi dilungare sul paradigma dell'Internet of Things, è evidente che sia necessario, per la tutela dei dati personali, fare ricorso alle PETs o, ancor più, ai concetti della Privacy by Design. Difatti, attraverso le PETs sarebbe necessario sfruttare le tecnologie per ridurre al minimo i rischi, ma è altrettanto possibile elaborare un progetto relativo all'IoT utilizzando i principi della PbD.

5. Tutela dei dati personali e profili tecnologici: dalle PETs alla Privacy by design.

L'evoluzione concettuale a cui si è fatto riferimento prima ha avuto riflessi sulle tecnologie e sulla loro applicazione alla tutela dei dati personali. Il primo riferimento è alle PET (acronimo di Privacy Enhancing Technologies) che, come si è accennato, in sintesi costituiscono le tecnologie utilizzate per garantire il diritto alla privacy. Ovviamente tali tecnologie vengono considerate in maniera neutra, ovvero senza alcuna connessione con specifiche fattispecie. Tale espressione fu utilizzata per la prima volta nel report pubblicato nel 1995 dal tiolo "*Privacy-enhancing technologies: the path to anonymty*", della Data Protection Authority olandese in collaborazione con il Commissario dell'Ontario (Canada). Il concetto di PET ha ricevuto diverse qualificazioni ed è stato oggetto di attenzione da parte della Commissione Europea soprattutto con il documento COM(2007) 228 costituito dalla Comunicazione della Commissione al Parlamento Europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)[2]. Tuttavia, già prima di tale comunicazione, la Commissione

[2] Cfr. Commissione delle comunità europee, *sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)*, documento COM(2007) 228, del 2 maggio 2007. Il testo è disponibile all'indirizzo

Europea nel 2004 con il documento COM(2003)265 “Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE)” al paragrafo 4.3 affermava testualmente: “*Le tecnologie PET (Privacy Enhancing Technologies) sono finalizzate alla concezione di sistemi e tecnologie di informazione e di comunicazione tali da ridurre al minimo la raccolta e l'uso dei dati personali e da contrastare forme illecite di trattamento. La Commissione ritiene che l'utilizzo di misure tecnologiche appropriate costituisca un complemento essenziale agli strumenti giuridici e dovrebbe costituire parte integrante di qualunque sforzo volto a conseguire un livello sufficiente di tutela della privacy*”.

Sul piano puramente pratico, il riferimento alle PET era rivolto a qualsiasi risorsa tecnologica che potesse ridurre i rischi di uso illecito dei dati personali. Peraltro, proprio a livello europeo il Seventh Framework Program (FP7), il programma europeo di finanziamenti per la ricerca e lo sviluppo tecnologico per il periodo 2007-2013, ha evidenziato l’importanza di adottare soluzioni tecnologiche per la protezione della privacy. Su questo fronte è chiara la voce del Garante europeo P. Hustinx che ha rilevato, invece, una mancanza di azione su questo fronte anche riguardo all’uso pratico delle PET in settori importanti.

Un esempio che frequentemente viene citato quando si discute di PETs e di anonimato in rete è quello noto il software Tor che “*è una rete di tunnel virtuali che permette alle persone ed alle organizzazioni di aumentare la propria privacy e sicurezza su Internet. Inoltre consente agli sviluppatori di software di creare nuovi strumenti di comunicazione con caratteristiche intrinseche di privacy. Tor fornisce le basi per una gamma di applicazioni con cui singoli individui ed organizzazioni possono condividere informazioni sulla rete pubblica senza compromettere la propria privacy*”[3].

Tuttavia, dalle PET negli anni ’90 il Commissario Privacy dell’Ontario ha iniziato a parlare di un nuovo concetto denominato

---

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:IT:PDF

[3] Questa è la definizione presente all’indirizzo a questo URL: http://www.torproject.org/overview.html.it

"Privacy by Design" che costituisce, in estrema sintesi, l'evoluzione delle PET senza abolirle, tant'è che si parla di PET Plus. In realtà, il profilo più delicato sul piano della riservatezza è costituito proprio dall'intero sistema IT e dalle comunicazioni mediante Internet. Privacy by Design si riferisce alla filosofia e all'approccio secondo cui la privacy va considerata nelle specifiche di progettazione delle varie tecnologie. Viene così prospettato che il concetto di Privacy by Design si estende alla seguente trilogia di applicazioni: "*Privacy by Design* now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure"[4]. In sostanza: 1) tecnologia dell'informazione; 2) pratiche commerciali responsabili; 3) progettazione delle strutture.

In particolare, con riferimento alla tecnologia dell'informazione si afferma, come già evidenziato, che la tecnologia non può costituire una minaccia per la privacy, ma un ausilio per la riduzione dei rischi. Per le pratiche commerciali responsabili, viene evidenziato come la privacy non va interpretata come un onere, un costo di gestione per le aziende ma, al contrario, come un vantaggio per una migliore competitività. Effettivamente, molte realtà aziendali considerano la privacy un costo inutile ed una serie di adempimenti del tutto inutili o comunque puramente burocratici; in realtà la conformità alla normativa privacy va considerata come un *quid pluris*, un valore aggiunto che incrementa la valutazione dell'azienda. Infine, l'elemento della progettazione delle strutture assume rilevanza – secondo il Commissario dell'Ontario – poiché molto spesso siamo costretti a vedere esposti i dati personali in aree pubbliche mal progettate come, ad esempio, le sale d'attesa degli ospedali o degli uffici, ove è possibile che vengano – illecitamente – divulgate le informazioni personali.

Al di là delle tre citate applicazioni, la *Privacy by Design*, per delineare gli ulteriori elementi schematici, si fonda su sette principi: 1) *Proactive not Reactive; Preventative not Remedial*; l'approccio alla PbD è di tipo proattivo piuttosto che reattivo; l'obiettivo è quello di anticipare gli eventi e non attendere che essi si verifichino per proporre rimedi alle soluzioni; 2) *Privacy as the Default:* questo

[4] http://www.privacybydesign.ca/

principio consiste nella salvaguardia del soggetto poiché il bene "privacy" va considerato a priori; in sostanza, nessuna azione è richiesta all'interessato per proteggere la propria privacy, perché i dati personali vengono protetti automaticamente in ogni sistema IT o commerciale, anche se il soggetto non fa nulla; 3) *Privacy embedded into Design*; la PbD è incorporata nell'architettura dei sistema e delle pratiche commerciali e non costituisce un *quid pluris*, un elemento da apporre successivamente: si tratta di una componente essenziale del sistema che non incide sulla sua funzionalità; 4) *Full Functionality – Positive-Sum, not Zero-Sum*; la PbD mira a conciliare tutti gli interessi legittimi e gli obiettivi in una somma positiva del tipo "win-win" dove sono inutili i compromessi e non attraverso un approccio datato del tipo "zero-sum"; in sostanza in un contesto tradizionale, un soggetto vince ed uno perde, mentre nella PbD tutte le parti devono risultare vincenti. Inoltre, "*Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both*"; 5) *End-to-End Lifecycle Protection*: incorporati i dati all'inizio non c'è rischio sino alla fine del processo di trattamento dei dati, con la sicurezza che, all'esito, tutti i dati saranno distrutti tempestivamente in modo sicuro. Così, la PbD assicura dalla culla alla tomba la gestione dell'intero ciclo vitale delle informazioni, "end-to-end"; 6) *Visibility and Transparency*: PbD garantisce che tutti i soggetti interessati, indipendentemente dalla prassi aziendale o dalla tecnologia, potranno in qualsiasi momento effettuare le verifiche più opportune in assoluta trasparenza; *Respect of user privacy*: al di là di tutto, la PbD richiede agli operatori che gli interessi dei soggetti siano preminenti e quindi offrendo misure come una forte privacy di default, informazioni appropriate e potenziando opzioni di facile utilizzo; il tutto con un approccio *user-centric*.

Come si può notare si tratta di una vera e propria rivoluzione della privacy che non concerne soltanto le misure tecniche per assicurare adeguata sicurezza ai dati personali, ma una serie di concetti innovativi che prescindono dall'assolutizzare la protezione dei dati personali per giungere alla considerazione che la sicurezza delle informazioni è insita nel concetto stesso di privacy. Se, ad esempio, si fa riferimento al principio n. 2) è evidente che un approccio di questo tipo sarà sicuramente più sicuro e vantaggioso per l'utente che non

dovrà più preoccuparsi per gli eventuali rischi dei propri dati personali: sarà necessario, al contrario, ridurre i livelli di privacy per una più ampia diffusione delle proprie informazioni. In ogni caso, l'intero assetto dei 7 principi fondamentali della PbD costituisce un vero e proprio programma per la tutela dei dati personali.

L'idea della Privacy by Design è stata recepita a livello europeo, tant'è che lo stesso Garante Europeo, P. Hustinx, l'ha fatta propria affermando la necessità di procedere mediante questa nuova fase indicando quale sicurezze tecnologiche proprio la p.b.d.[5] Ma lo stesso Garante europeo precisa che il concetto di Privacy by Design non rileva solo per il sistema tecnologico, ma anche per le organizzazioni e i metodi in generale e così anche per una maggiore efficienza delle data protection authorities[6].

6. Conclusioni.

Pertanto, in conclusione, il quadro che si va delineando a livello europeo ed internazionale è di una evidente evoluzione del concetto di privacy e delle tecnologie a supporto. Non va, tuttavia, dimenticato che l'attuale assetto normativo europeo[7] e, conseguentemente quello nazionale con il codice privacy (art. 31 e segg.), impone l'utilizzo di misure tecniche ed organizzative appropriate con un evidente richiamo alle PET. I fenomeni descritti all'inizio di questo contributo costituiscono soltanto un esempio di ciò che si può verificare nel sistema delle comunicazioni e di quale rilevanza assumano i dati personali. PbD può essere uno dei canali attraverso cui veicolare l'approfondimento e la protezione dei dati personali. Le PET non vanno, quindi, considerate come una soluzione obsoleta, ma quale strumento sinergico del concetto più evoluto di Privacy by Design, proprio ove si vuole rimarcare la necessità di pensare alla privacy sin dalla progettazione di un sistema. Infatti la PbD, come si è accennato,

[5] Cfr. P. HUSTINX, *More effective Data Protection: "facing up to a digital world"*, 2.6.2010, Bruxelles

[6] Cfr. P. HUSTINX, *Privacy by design: delivering the promises*, in *Identity in the Information Society*, vol. 3, n. 2, 2010.

[7] Cfr. Direttiva 95/46/EC, art. 17.

viene definita come PET Plus, proprio ad indicare il valore aggiunto alle PET. L'approccio alla PbD denota come, sul piano ontologico, si discuta di concetti assolutamente innovativi anche rispetto alla nostra cultura giuridica che non ha trascurato di considerare il diritto alla riservatezza come uno dei diritti fondamentali dell'individuo. Ma l'analisi della PbD lascia arguire anche un approccio più distaccato dal dato normativo, poiché piuttosto che riconoscere la rilevanza (giuridicamente) della privacy e quindi della tutela dei dati personali, l'individuo diventa (così come si esprime il principio n. 7) il fulcro del sistema. Difatti, l'approccio *user-centric* fa chiarezza sui principi della PbD nel senso che essa vada considerata ontologicamente come elemento essenziale nella sfera dell'individuo. Ritengo che, a maggior ragione, non si possa prescindere (come correttamente ha fatto il legislatore italiano) dalla considerazione della PbD anche per la tutela delle persone giuridiche.

Ciò, a mio modesto avviso, non deve preoccupare il giurista per l'apparente distacco della privacy dal supporto normativo a favore di un approccio di tipo idealistico volto all'esaltazione dei principi generali. In realtà, le caratteristiche della PbD non pregiudicano il dato essenziale e contenutistico della privacy e non la lasciano priva di tutela. Infatti, la PbD arricchisce il concetto di privacy e comunque soggiace alle valutazioni sulla idoneità ad essere meritevole di tutela secondo l'ordinamento giuridico (non può escludersi che nel campo dei diritti la valutazione si possa spostare su altro profilo quale, ad esempio, quello della persona o addirittura sul piano più alto dei diritti fondamentali dell'individuo). Probabilmente i tempi non sono ancora maturi per discutere appieno di Privacy by Design, ma è opportuno che si cominci a riflettere sulla validità di tale concetto rispetto alla privacy e alla protezione dei dati personali, soprattutto con riguardo a quelli sensibili.

Google, Street View, and Privacy: An Objective Look from Europe

di Paolo Balboni *

SUMMARY: 1. Introduction. – 2. Setting the scenario: some facts and figures. – 3. "Is this a conspiracy behind Street View or is this concern somehow justified? What happened exactly?" – 4. "What does this collection of information, personal, and possibly sensitive data has to do with the provision of the service 'Street View'?" – 5. Focusing on the issue and the way forward.

1. Introduction.

As member of the European Privacy Associations ("EPA")[1], board member of the Italian Institute for Privacy[2], ICT lawyer and academic[3] I was asked to comment on the privacy and data protection issues raised by Street View in Europe at an open event hosted by Big Brother Watch in Westminster central London on Tuesday 20 June 2010. In this short article I will: (i) briefly analyse the matter; (ii) confront with the other authors who have taken part in the relevant debate on the dedicated section of the website *Spiked* [4] – yet staying away from any polemic on whether or not Google has to be

* Attorney at law in Milan, specialized in ICT law and personal data protection; Istituto Italiano per la Privacy. All the Internet addresses quoted in this article were last visited on 16 July 2010.

[1] See European Privacy Association website available at the following Internet address: <www.europeanprivacyassociation.eu>.

[2] See Italian Institute for Privacy website available at the following Internet address: <http://www.istitutoitalianoprivacy.it/en/>.

[3] See Paolo Balboni's personal website available at the following Internet address: <www.paolobalboni.eu>.

[4] See Spiked: "Google and Privacy. Is the Web Giant Invading our Private Lives", available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_home/>.

considered 'evil'; and (iii) propose some recommendations for the future.

2. Setting the scenario: some facts and figures.

Six hundred gigabytes of data were collected by Google cars in thirty-three countries around the world for the Street View service[5]. Since then, nine EU member states (Austria, Belgium, Czech Republic, Denmark, France, Germany, Ireland, Italy, Spain, Switzerland) have acted, mainly through their Data Protection Authorities ("DPAs"), to stop Google cars' unlawful collection of personal data. Some of them asked Google to freeze said data during the investigations, others ordered the immediate destruction of the data collected. Both the Italian and the French DPAs, explained in their respective speeches when presenting their annual reports[6] that Google cars collected not only information on Wi-Fi connections but also the content of communications[7]. Moreover, French DPA president Alex Türk explained that he was willing to set an example with Google in order to make companies understand that as soon as

[5] See G. MARINO, *Il Grande Fratello Informativo. Quanti nemici per Google. L'Europa ora indaga sui dati intercettati nei pc*, il Giornale, 24 May 2010, p. 12.

[6] The Annual Report presentation speech of the Italian DPA president is available at the following Internet address: <http://www.garanteprivacy.it/garante/document?ID=1730115>. The Italian DPA Annual Report is available at the following Internet address: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1730032>. The Annual Report presentation speech of the French DPA president is available at the following Internet address: <http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/rapport-annuel-defis-et-perspectives-2010/>. The French DPA Annual Report is available at the following Internet address: <http://www.cnil.fr/uploads/media/CNIL-30erapport_2009.pdf>.

[7] See the Italian DPA press release on 19 May 2010 "Il Garante privacy avvia istruttoria su Google Street View", available at the following Internet address: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1720935>. See the French DPA press conference on 17 June 2010 "Présentation du 30ème rapport d'activité 2009", available at the following Internet address: <http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL_DP-conference-presse_17-06-2010.pdf>.

they are dealing with private data, their liability can be engaged, and that it is not sufficient to delete data afterwards.

3. "Is this a conspiracy behind Street View or is this concern somehow justified? What happened exactly?"

For any conclusive comment we should first await the conclusion of the running investigations. However, while waiting, we, at EPA, have asked a respected computer engineer to give us some technical details on the matter, to help us gain a better understanding of the affair. He explained that if Google cars are driving around capturing Wi-Fi packets and cataloguing them, while they are photographing for Street View, one would expect Google to be able to catalogue several things:

1. The geo-coordinates of where they picked the packet up. That is, they tie each picture/view to geo-coordinates (longitude and latitude), an azimuth (compass direction that the camera was pointing while at the geo-coordinates), and an elevation (how far up or down the camera is pointing).
2. The source and destination IP address of the packet. Since they pull the packets out of the air instead of a wire, 99% of the packets are going to be traffic between a PC or terminal device and a wireless router. Some of the traffic is going to be Wi-Fi router-to-Wi-Fi router (one can chain them together), and some is going to be PC-to-PC (two PCs can talk via Wi-Fi without a router in between). But the bulk is going to be between a PC/terminal and a Wi-Fi router.
3. Of that 99% of the traffic, they are going to get the MAC addresses of the devices -- the PC and the Wi-Fi router. That is going to map, for the most part, to the Ethernet ports, but 'usually' uniquely identifies the device. 'Usually', because an Ethernet port can have more than one MAC address. Once the packet gets to the Wi-Fi router, the PC's MAC address disappears from the packet.
4. The network ID of the Wi-Fi network (SSID).
5. What kind of encryption the two devices (PC and router) are running.

6. If the link is not encrypted, they are going to see all kinds of things, like what protocols the people on that network are running, and precisely what they are doing. They probably see a lot of unencrypted Wi-Fi hotspots, which means they are seeing a lot of unencrypted traffic. In principle, there are a lot of things they could do with that. Metaphorically speaking, it is exactly as if they were standing over one's shoulder recording every keystroke and everything that comes up on your screen. Potentially, they are going to be seeing people's emails, chat sessions, business documents, medical or bank details, picking up video feeds from Wi-Fi camera and/or some audio in the form of VoIP.

In the end, their database is going to include the geo-coordinates, the date and time of the interception, the to/from IP addresses, the to/from MAC addresses, information on what types of devices those are, the network ID, how many devices are on that net at that particular time, how far that network extends in terms of distance, whether it is encrypted, and, if it is, what type of encryption they're using, what protocols are in use between the two devices (if unencrypted), and the actual content of messages (if unencrypted). Statistically, one could argue that they would know as much about how/why/where/when people surf.

4. "What does this collection of information, personal, and possibly sensitive data has to do with the provision of the service 'Street View'?".

Actually, it seems quite clear that in order to provide a service that should primarily consist of displaying streets and places to users, Google does not need to collect data concerning how/why/where/when people surf in those locations. This brings about the preliminary legal conclusion that the data collected are not proportionate to the scope of the processing - one of the main principles set fort in the EU Directive 95/46/EC[8]. Moreover, in order

[8] See 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

to lawfully collect such data Google, as a general principle, should have informed the data subjects and obtained their prior consent. Given that this did not happen, the data processing carried out by Google has been unlawful, as a number of European DPAs have already stated in their preliminary conclusions to their Street View investigations. Google asserted that it was an accident, apologized, and has promptly started to cooperate with the authorities. It is an accident of serious proportion when a company sends cars out to collect pictures of streets and places and they return with the contents of communication, which are not only protected by data protection law (and its fundamental principle that individuals should be able to control their use of personal information) but also by the right of privacy and confidentiality of correspondence – a constitutional right in most of the EU Member States. This challenges what Google Director of communication and public affairs for North and Central Europe Peter Barron wrote in his debate contribution "We believe in the principles of transparency and choice and aim to design products that give users meaningful choices about how they use our services and what information they share with us"[9].

I agree with Director of the Enterprise Privacy Group Toby Stevens when he writes that it is the uncertainty of not having heard all the truth around Street View that worries him the most, that is, "the possibility that one of the world's largest companies is allegedly aggregating personal information and not being transparent about its motives" – considering that this is an "accident that happened for three years in 30 countries, supported by a patent application for the collection process"[10].

Personal Data and on the Free Movement of such Data, *Official Journal* L 281 , 23/11/1995 p. 0031 – 0050.

[9] See P. BARRON, *Privacy is a Priority. Our Business Depends on It*, Spiked, 28 June 2010, available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_article/9090/>.

[10] See T. STEVENS, *Why It's Time for Google to Open up*, Spiked, 6 July 2010, available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_article/9167/>.

Moreover, Peter Barron wrote that "[w]ithin Google we have experienced lawyers whose sole focus is to address these issues"[11]. I trust Google has among the best lawyers of the world, and I say: "Use them!" or "Listen to them!". A first-year law student would have spotted the problems Google are now encountering. I agree with Simon Davies (Director of Privacy International) when he writes that he "want[s] to see every Google product risk-assessed (…) [and] subject to a privacy checklist"[12]. My experience as a business lawyer tells me that this is actually what does happen at most of the mature, large ICT companies.

"Privacy cannot be sidelined in the rush to introduce new technologies to online audience around the world"[13] rightly stated ten Data Protection Commissioners in their open letter to Google CEO Eric Schmidt on 19 April 2010, commenting on Google Buzz (and incidentally on Street View). They also stressed that they "remain extremely concerned about how a product with such significant privacy issues was launched in first place"[14].

Furthermore, Barrister and Director of Big Brother Watch Alex Deane pointed out in his article that "Google takes masses of pictures of us and our property without our consent and without giving us notice, and then tells us that if there are problems, it's up to us to identify them. This gets things the wrong way round. It's *Google*'s responsibility, but its representatives respond that an opt-in system makes Google Street View unworkable."[15] Now I fully understand that an opt-in system, where Google has to gain the consent of those affected by the pictures, would have made Google Street View unworkable. However, the implementation of new business ideas is

[11] See P. BARRON, *Privacy is a Priority*, *op. cit.*

[12] See S. DAVIES, *Google Has Become an Imperialist Beast*, Spiked, 28 June 2010, available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_article/9089/>.

[13] Available at the following Internet address: <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf>.

[14] Id.

[15] See A. DEANE, *A Systematic Intrusion into People's Lives*, Spiked, 6 July 2010, available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_article/9168/>.

often stopped (or slowed down) by legal issues. This is because regulations are issued precisely to prevent a wild and uncontrolled development of businesses and services – even when they may be useful – that may breach fundamental rights and freedoms. Given what has recently been discovered about Street View, I think it is normal and sound at this point to stop for a moment (or slow down) the implementation of Street View. As Conservative MP Robert Halfon said "There's a great difference between advancement of the internet and violating people's right to privacy"[16].

5. Focusing on the issue and the way forward

One problem must be acknowledged. Laws and regulations on ICT services are far from being globally uniform. Objectively, it is very challenging (if not impossible) for a global innovative ICT company to comply with all the applicable laws in the world and to keep their business up and running at a fast peace. As far as data protection is concerned, more and more services are encountering numerous compliance issues related to the absence of global data protection rules/standards. For example, one should consider cloud computing services, a market that is significantly expanding, in which a number of big players are involved (e.g., Amazon, Google, Microsoft, SalesForce, IBM, etc.). In my view, big companies should stop fighting each other on the issue of privacy – as it has recently become a popular sport. It would be more beneficial both for them and for the users if such companies start to work out best practices together with DPAs and Privacy Commissioners around the world, with the aim of setting out workable international privacy standards. For example they could start to work on a practical and detailed explanatory memorandum for the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution)[17]. Google, in its

[16] See R. HALFON, *Google is Watching You!*, Spiked, 12 July 2010, available at the following Internet address: <http://www.spiked-online.com/index.php/debates/google_article/9189/>.

[17] International Conference of Data Protection and Privacy Commissioners (5 November 2009) *International Standards on the Protection of Personal Data and*

position as a world champion ICT business, could actively promote these activities, thereby setting the example. Once agreed upon, international privacy standards could be embedded directly into companies' products and services following the very valuable concept of Privacy by Design. In fact, the Article 29 Working Party has recently proposed to include this, together with 'Accountability', as principles in the EU legal framework of data protection[18].

In the meantime I think we all hope that Google, as well as all organizations entrusted with people's personal information, will follow the recommendation issued by the ten Data Protection Commissioners in their open letter to Eric Schmidt "to incorporate fundamental privacy principles directly into the design of new online services. That means, at a minimum:

- collecting and processing only the minimum amount of personal information necessary to achieve the identified purpose of the product or service;
- providing clear and unambiguous information about how personal information will be used to allow users to provide informed consent;
- creating privacy-protective default settings;
- ensuring that privacy control settings are prominent and easy to use;
- ensuring that all personal data is adequately protected; and
- giving people simple procedures for deleting their accounts and honouring their requests in a timely way."[19].

Privacy (The Madrid Resolution), available at the following Internet address: <http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf>.

[18] See ARTICLE 29 Data Protection Working Party, The Future of Privacy. *Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, adopted on 1 December 2009, available at the following Internet address: <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf>.

[19] Available at the following Internet address: <http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf>.

Intercettazioni telefoniche e telematiche: un giusto equilibrio tra privacy, giustizia ed informazione

di Michele Iaselli [*]

SOMMARIO: 1. Introduzione. – 2. Situazione normativa. – 3. La tutela della riservatezza. – 4. Contrasto tra esigenze di giustizia e di informazione. Una possibile soluzione.

1. Introduzione.

Da che mondo è mondo, se qualcuno ha una conversazione privata può darsi che qualcun altro tenti di spiarla. Quando le faccende importanti si discutevano nei salotti, le spie si appostavano dietro una tenda e tendevano l'orecchio per sentire che cosa si diceva. Poi, quando le conversazioni si sono spostate sul telefono, sono stati messi sotto controllo i fili. E oggi che tante attività umane si svolgono nel cyberspazio le spie si sono infiltrate *on line*. Come è noto la materia delle intercettazioni telefoniche è diventata negli ultimi tempi molto delicata ed è assurta agli onori della cronaca a seguito delle proposte del Governo di modificare il "regime" delle intercettazioni telefoniche e di limitare la possibilità di divulgare notizie sulle stesse. Diversi sono gli interessi in gioco tutti di rilevanza costituzionale quali la privacy dei cittadini, la fondamentale esigenza di giustizia che deve garantire la magistratura e il diritto all'informazione rivendicato dalla categoria dei giornalisti.

Cerchiamo adesso di capire se è possibile trovare un giusto equilibrio tra tanti interessi degni tutti di tutela ma che non possono sfuggire all'inevitabile principio del "pari rango". Le intercettazioni telefoniche sono certamente necessarie per le indagini, ma non tutte le indagini necessitano dell'uso dello strumento delle intercettazioni.

[*] Avvocato, Presidente dell'Associazione Nazionale per la Difesa della Privacy; Istituto Italiano per la Privacy.

Peraltro, se l'eventuale abuso d'indagine incide, come è ovvio, su diritti fondamentali del cittadino (*in primis* quello sancito dall'art. 15 della Costituzione, laddove è prescritto che *"la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili"*), assai più pericoloso e dannoso è l'uso distorto che sovente viene fatto, attraverso la pubblicazione sulla stampa, delle trascrizioni delle intercettazioni.

Da tempo si tenta una ragionata revisione della disciplina delle intercettazioni. Ed indubbiamente ben venga. Sono anni che si conoscono i limiti delle norme vigenti, molte proposte erano state avanzate e costituiscono una buona base per definire con maggior precisione i casi in cui le intercettazioni sono ammesse; le loro modalità; i criteri di selezione, utilizzazione e conservazione del materiale raccolto; il rapporto tra segretezza dei contenuti delle intercettazioni e loro pubblicità. Sembra che si stia acquisendo piena consapevolezza del fatto che, in ogni caso, le intercettazioni sono uno strumento d'indagine che porta con sé rischi elevati per le libertà delle persone. Come è stato giustamente sostenuto ogni modifica legislativa, però, deve avere una portata generale, con una giusta preoccupazione per tutti i soggetti e le conversazioni non direttamente rilevanti per le indagini. Se non si affronta il problema in questo modo, si rischia di avere sì una nuova disciplina, ma questa assomiglierà piuttosto ad una rete di protezione per alcune categorie di persone e di reati, per non dire ad una riforma "punitiva", che non ad una effettiva garanzia per tutti. Il rischio è reale. Alla improvvisa attenzione per nuove norme si è giunti sulla spinta delle polemiche suscitate da intercettazioni "eccellenti", non partendo dai molti casi dubbi di questi anni. Non si devono delegittimare anche le intercettazioni rilevanti, e chi le ha disposte e utilizzate, se davvero si vuole arrivare ad una seria riforma. Si continua a parlare di pubblicazioni illegittime, ignorando i pazienti chiarimenti venuti da seri studiosi della procedura penale che, tra l'altro, hanno messo in evidenza come il segreto venga meno per tutte quelle parti delle

intercettazioni citate negli atti giudiziari comunicate a tutti i soggetti interessati[1].

2. Situazione normativa.

Ma vediamo in sintesi qual è il quadro normativo esistente e quello probabilmente futuro. Come è noto, l'intercettazione è *"consentita"*, previa autorizzazione concessa con decreto motivato al P.M. dal G.I.P., solo in relazione a ben delimitate gravi ipotesi delittuose (analiticamente indicate dall'art. 266 c.p.p.) e solo *"quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini"* (art. 267 c.p.p.). Il nuovo Esecutivo ha presentato un diverso Disegno di Legge, che addirittura dovrebbe essere destinato a restringere ulteriormente la possibilità di disporre intercettazioni telefoniche sempre che sussistano i gravi indizi di colpevolezza a carico dell'indagato nei cui confronti la intercettazione deve essere effettuata (non sarebbe più sufficiente verificare la sussistenza del reato ma occorrerebbe verificare anche la responsabilità del soggetto). Inoltre sarebbero introdotte sanzioni severissime per la pubblicazione del contenuto delle intercettazioni da parte dei giornalisti. In particolare le intercettazioni diventano possibili solo nel caso di reati puniti con più di cinque anni di reclusione (ad esempio, reati contro la Pubblica amministrazione, stalking). I telefoni possono essere messi sotto controllo per un massimo di 75 giorni ma, se ve n'é la necessità, possono essere concessi altre 72 ore prorogabili, di volta in volta, previa autorizzazione del tribunale collegiale, qualora esistano elementi fondanti per l'accertamento del reato o indicazioni rilevanti per impedire la commissione di un reato.

Per i reati più gravi (come, ad esempio, mafia, terrorismo, omicidio ecc.) le intercettazioni sono possibili per 40 giorni, ma possono essere prorogate dal tribunale con decreto motivato per periodi successivi di

[1] Cfr. E. APRILE, *Sulla utilizzabilità delle intercettazioni disposte in altri procedimenti anche nel caso di omesso deposito degli atti relativi*, in *Cassazione Penale*, n. 3, 2010, 1028.

venti giorni, qualora permangano gli stessi presupposti, entro i termini di durata massima delle indagini preliminari. Gli atti delle indagini in corso non possono essere pubblicati tra virgolette ma solo in forma di riassunto, sempre che si tratti di atti non più coperti da segreto. Nel caso di pubblicazione testuale, gli editori possono essere puniti con la multa fino a 300mila euro. Le intercettazioni non possono essere pubblicate, nemmeno per riassunto, fino alla conclusione delle indagini preliminari, anche se non più coperte da segreto istruttorio: in caso contrario gli editori sono punibili con la pena della multa di 300 mila euro, che può salire fino a 450 mila euro nel caso in cui vengano intercettate persone estranee ai fatti o di intercettazioni destinate alla distruzione (ovvero di conversazioni ininfluenti ai fini dell'inchiesta).

Per quanto riguarda i giornalisti, questi rischiano fino a 30 giorni di carcere o una sanzione fino a 10.000 euro nel caso di pubblicazione di intercettazioni durante le indagini o di atti coperti da segreto. Dal punto di vista normativo, la possibilità di pubblicare le trascrizioni delle intercettazioni eseguite in modo legittimo incontra, innanzitutto, i limiti sanciti dallo stesso codice del rito penale, in modo particolare dagli artt. 114 c.p.p. (che disciplina il divieto di pubblicazione degli *atti coperti da segreto* ovvero di *quelli non piu' coperti da segreto*, consentendo invece la pubblicazione del contenuto degli atti *non coperti dal segreto*), 115 c.p.p. (che, in aggiunta alla sanzione penale, impone la trasmissione degli atti all'organo titolare del potere di instaurare *l'azione disciplinare*) e 329 c.p.p. (che indica quali sono gli atti coperti da segreto, prevedendo la ulteriore possibilità per il P.M. della *secretazione* in caso di necessità d'indagine).

Il Disegno di Legge n. 1638, predisposto dall'allora ministro Mastella ed approvato il 17.4.2007 da uno solo dei rami del Parlamento, era destinato ad estendere il divieto di pubblicazione fino alla conclusione delle indagini preliminari ovvero fino al termine dell'udienza preliminare.

Per le intercettazioni acquisite in modo illegale, è intervenuto il Decreto Legge 22.9.2006 n. 259 convertito nella legge 20.11.2006, n. 281, che ne ha regolamentata la distruzione, disciplinando le conseguenze penali e risarcitorie del loro illecito uso.

3. La tutela della riservatezza.

Quanto, invece, al versante della tutela della riservatezza dei dati personali, parecchie disposizioni sono rinvenibili nel testo del D.Lgs. 30.6.2003 n. 196 (c.d. "Codice della Privacy"). Il Titolo I, nello stabilire quale principio generale che "chiunque ha diritto alla protezione dei dati personali che lo riguardano" (art. 1), prevede che il trattamento "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" (art. 2), intendendosi come dato personale "qualunque informazione relativa a persona fisica, persona giuridica,ente o associazione,identificati o identificabili,anche indirettamente,mediante riferimento a qualsiasi altra informazione" (art. 4 lett. b) ivi compresi i *dati giudiziari*, anche solo rivelatori della "qualità di imputato o di indagato" (art. 4 lett. e).

Il Titolo III, nell'indicare le regole per il trattamento dei dati, prevede che il rispetto di quelle che sono contenute nei "Codici di Deontologia" (ivi compreso quello dei giornalisti) "costituisce condizione essenziale per la liceità e correttezza" del trattamento stesso (artt. 3-4).

Il Titolo XII, nel disciplinare le regole attinenti l'attività giornalistica, dispone che il Codice di Deontologia relativo al trattamento dei dati debba prevedere *"misure e accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quelli idonei a rivelare lo stato di salute e la vita sessuale"* e che in caso di violazioni delle prescrizioni contenute nel Codice stesso *"il Garante può vietare il trattamento"* (art. 139).

Pur prevedendo, inoltre, l'esenzione da alcune restrizioni previste per altre categorie (ad esempio, in materia di dati giudiziari), stabilisce che, in ogni caso, debbano restare*"fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'art.2 e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico"* (art. 137).

Il Garante, nell'ipotesi accertata di violazioni del Codice della Privacy (e del Codice Deontologico), può adottare una serie di misure che varia dal blocco al divieto totale o parziale del trattamento (art.

143), che può essere preceduta dalla prescrizione, anche d'ufficio, di ogni cautela opportuna (ivi compreso il divieto o il blocco del trattamento dei dati: art. 154). La stessa Autorità è più volte intervenuta in materia ribadendo il principio secondo cui la pubblicazione di dati giudiziari (art. 4, comma 1, lett. *e*) del Codice) è ammessa anche senza il consenso dell'interessato, ma nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; art. 12 del codice di deontologia), nonché nella misura in cui i dati non siano relativi ad atti coperti da segreto o non pubblicabili per legge (art. 114 c.p.p.). L'essenzialità dell'informazione deve essere valutata caso per caso, nel contesto dei fatti narrati (art. 6 del codice di deontologia). Con un provvedimento generale del 21 giugno 2006 l'Autorità ha richiamato l'attenzione di tutti gli operatori sulla necessità di assicurare, anche nel legittimo esercizio del diritto di cronaca su fatti di interesse pubblico, una tutela adeguata dei diritti di soggetti coinvolti, anche indirettamente, in tali conversazioni. Ciò, a maggior ragione atteso che le intercettazioni possono riguardare conversazioni intercorse con terzi estranei ai fatti oggetto di indagine penale o non ancora indagati; conversazioni su relazioni personali o familiari, o su persone lese dai fatti; oppure, infine, conversazioni che attengono a comportamenti strettamente personali di soggetti pur coinvolti nelle indagini, ma non direttamente collegati a fatti penalmente rilevanti.

Il Garante ha nuovamente rilevato che i mezzi di informazione devono rispettare alcune regole già indicate nel codice di deontologia: l'informazione, anche dettagliata, può essere diffusa solo se risulta indispensabile per l'originalità dei fatti a cui si riferisce, ovvero per la qualificazione dei protagonisti di tali fatti o per la descrizione dei modi particolari in cui essi sono avvenuti (art. 6, comma 1, del codice di deontologia); devono essere evitati riferimenti a congiunti o ad altri soggetti non interessati ai fatti (art. 5, comma 1, del codice di deontologia); deve essere comunque assicurato il pieno rispetto della dignità della persona, nonché della sfera sessuale dei soggetti coinvolti, astenendosi in particolare da descrizioni su abitudini sessuali; infine, quando le informazioni riguardano individui che rivestono una posizione di particolare rilevanza sociale o pubblica, devono comunque essere rispettati sia il principio dell'essenzialità

dell'informazione, sia la dignità personale. Ma con il predetto provvedimento il Garante ha posto altresì in evidenza l'insoddisfacente quadro normativo relativo all'utilizzabilità in sede extraprocessuale di atti processuali e, in particolare, delle trascrizioni di conversazioni intercettate. In tale prospettiva l'Autorità ha anche nuovamente segnalato al Ministero della giustizia e al Consiglio Superiore della magistratura l'esigenza di migliorare tali meccanismi e tutele.

4. Contrasto tra esigenze di giustizia e di informazione. Una possibile soluzione.

Da troppo tempo ormai il nostro Paese ha riconosciuto a *magistrati* e *giornalisti* il merito e la capacità di mettere in luce interi settori inquinati della vita civile ed istituzionale: l'inevitabile conseguenza è che si rinnova l'immancabile rituale delle reciproche accuse, soprattutto quando l'oggetto del contendere è rappresentato dalla attuazione e dalla pubblicazione delle intercettazioni telefoniche[2]. Ognuno imputa all'altro violazioni di norme di legge ovvero del senso della misura, invocando la corretta applicazione delle regole del diritto e della deontologia professionale. Le ragioni della magistratura vengono, spesso, racchiuse nel seguente assioma: le intercettazioni di conversazioni o comunicazioni telefoniche, oltre che previste e disciplinate dalla legge, sono mezzi di ricerca della prova insostituibili nell'epoca moderna, nella quale sovente chi delinque non lascia ulteriori tracce dei propri comportamenti. Le ragioni del giornalismo sono solitamente riassumibili nel presunto obbligo deontologico di dover pubblicare tutto il materiale in qualunque modo acquisito, allo scopo di rispettare quella sorta di patto etico stipulato con i lettori, che impone la rivelazione della realtà e della verità, ancor piu' dovuto quando sono coinvolte nei fatti persone di rilievo pubblico.

[2] Cfr. G. GIOSTRA, *Intercettazioni: troppo vago l`interesse da tutelare per allontanare i dubbi di illegittimità sulla norma,* in *Guida al diritto,* n. 31, 2009, 10 e ss.

Diventa indispensabile, a questo punto, chiarire quali sono le regole che devono presiedere l'attività dei giudici e alla conservazione da parte dei giudici delle informazioni che acquisiscono a fini di giustizia. Sono informazioni che possono essere comunicate ai cittadini e divenire oggetto di informazione nei limiti in cui sono rese conoscibili. A fronte di tale considerazione va sottolineata la responsabilità etica e deontologica del giornalista e del direttore che devono valutare l'interesse pubblico a conoscere ed evitare di ledere inutilmente la dignità della persona, si tratta di un problema che rimane legato alla deontologia professionale.

Nel conflitto, quindi, tra interessi egualmente garantiti dalla Costituzione, il bilanciamento tra il diritto alla riservatezza ed il diritto di informazione non pare, però, suscettibile di soluzioni aprioristiche ovvero di una qualsivoglia minuziosa codificazione di regole preventive[3]. In effetti, la molteplicità e la varietà delle vicende di cronaca e dei soggetti che ne sono coinvolti non consentono di stabilire *ex ante* ed in modo categorico quali particolari e quali notizie possano essere raccolti e diffusi. Spesso, anzi, la pubblicazione che appare legittima in un determinato contesto, non potrebbe esserlo in un contesto diverso. Come si è visto questo bilanciamento tra i diritti e le libertà di cui sopra resta in sostanza affidato in prima battuta al giornalista, ma il pericolo è che spesso anziché il diritto all'informazione venga privilegiato l'interesse, non altrettanto nobile e tutelato, al c.d. *gossip* ovvero, il che è ancor peggio, alla più crudele curiosità legata alle miserie altrui, soprattutto se *l'altro* è un personaggio pubblico. I rischi di una regolamentazione legislativa delle intercettazioni telefoniche sono evidenti. Difatti in un Paese nel quale l'illegalità, soprattutto dei *colletti bianchi*, sembra moltiplicarsi in modo esponenziale, invocare un drastico ridimensionamento dello strumento d'indagine delle intercettazioni suonerebbe come un segnale di resa o di rassegnazione alla criminalità d'*élite*[4]. Parimenti, il diritto-dovere di informare e di essere informati potrebbe essere

[3] Cfr. V. MAFFEO, *La riforma in itinere delle intercettazioni, tra tutela della privacy ed esigenze dell`accertamento*, in *Diritto Penale e processo*, n. 4, 2009, 510 e ss.
[4] Cfr. M. L. DI BITONTO, *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *Cassazione penale*, n. 1, 2009, 8.

vanificato da astratte previsioni limitative, magari dettate dall'indignazione estemporanea di qualche potentato.

L'impressione è che a prescindere da drastici interventi di carattere normativo il giusto equilibrio tra necessità investigative, diritto di informazione e tutela della privacy può essere assicurato innanzitutto dal rispetto, da parte dei magistrati, delle limitazioni di legge in materia di intercettazioni e l'utilizzo di tale strumento d'indagine solo in ipotesi di concreta ed effettiva necessità, ne costituirebbero il necessario presupposto. Peraltro la normativa vigente già richiederebbe (ma la norma non è sempre rispettata) la trascrizione delle sole conversazioni rilevanti per l'oggetto del processo, con la esclusione di tutte quelle riguardanti vicende personali non pertinenti (il 6° comma dell'art. 268 c.p.p. dispone che il giudice non acquisisca le conversazioni "manifestamente irrilevanti"). La stessa disposizione prevede lo stralcio anche dalla registrazione delle conversazioni di cui è vietata la utilizzazione[5]. Inoltre, l'effettivo adeguamento, da parte dei giornalisti, ai principi stabiliti nel Codice della Privacy e nel Codice Deontologico, ne rappresenterebbe il giusto completamento.

[5] Cfr. A. BALSAMO, *Intercettazioni: gli `standards` europei, la realtà italiana, le prospettive di riforma*, in *Cassazione penale*, n. 10, 2009, 4025

Privacy ed equilibri strategici nel cyber-spazio

di Stefano Mele [*]

SOMMARIO: 1. Introduzione. – 2. La protezione delle infrastrutture critiche nazionali dagli attacchi portati attraverso la rete Internet. – 3. La tecnologia a difesa della Rete. – 4. Le norme a difesa dei cittadini. – 5. Conclusioni.

1. Introduzione.

L'accostamento del concetto di privacy a quello di sicurezza nazionale fa pensare, da un po' di anni a questa parte, ad un vero e proprio ossimoro, piuttosto che a una semplice (forse meramente ipotetica) antitesi. Troppe volte in questo decennio, in particolar modo dal 2001 in poi, si è diffusa l'idea che in nome del baluardo della sicurezza nazionale – concetto di ampia focalizzazione e spesso di difficile verificazione – il diritto giustissimo alla privacy e alla protezione dei dati personali dei cittadini fosse stato da più parti compresso, se non addirittura compromesso. Voltandoci indietro, però, pare, oggi, addirittura futile affermare che nella realtà delle cose, almeno in Italia, quanto da più parti profetizzato fortunatamente non si è mai avverato[1]. Dopo l'11 settembre 2001, infatti, non ci sono state nel nostro Paese evidenti scollature tra le libertà personali, quindi anche quelle relative alla privacy e alla protezione dei dati personali, e le esigenze di difesa nazionale, come invece è avvenuto in America[2] e

[*] Avvocato specializzato in Diritto delle Tecnologie Informatiche, Privacy, Sicurezza e Intelligence; Istituto Italiano per la Privacy.

[1] Questo soprattutto grazie all'occhio attento e all'attività incessante del Garante per la protezione dei dati personali, nonché degli studiosi e delle associazioni operanti in questo settore.

[2] H.R.3162, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)*, 2001, reperibile in Rete su http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:
Sul piano strettamente tecnologico, invece, sempre l'America provò a far passare in maniera molto rapida un progetto particolarmente dettagliato e completo denominato

in alcuni Paesi europei[3]. In questo senso le uniche variazioni normative degne di significato sono state quelle relative all'estensione delle intercettazioni preventive delle comunicazioni[4] per i delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale e quelle del 2005 derivanti dal dettato del c.d. "Decreto Pisanu"[5].

Total Information Awareness (TIA), subito ribattezzato dall'*Electronic Privacy Information Center* (EPIC) "*Terrorism Information Awareness*", rimasto però solo un progetto.

[3] Soprattutto Gran Bretagna, Germania, Svezia e Danimarca.
In particolare in Germania, all'indomani degli avvenimenti dell'11 Settembre 2001, non fu approvata una proposta di legge, in quel periodo in una fase avanzata di discussione, particolarmente liberale nei confronti dell'immigrazione, laddove, all'opposto, furono adottati immediatamente parametri più rigidi nella legislazione che regola la libertà di circolazione dei cittadini. Inoltre, sia in Germania che in Gran Bretagna furono adottati nuovi sistemi di identificazione digitale dei cittadini con lo scopo di rafforzare la sicurezza e i controlli alle frontiere. Infine, in quasi tutti gli Stati occidentali furono introdotti strumenti legislativi volti a prolungare la conservazione delle comunicazioni elettroniche e a garantire la possibilità di analisi del *clickstream*, ovvero del comportamento di un utente all'interno di un sito (i suoi spostamenti fra diverse pagine, il tempo di permanenza su una specifica pagina, immagini e testi selezionati o scaricati sul proprio computer, ecc.).

[4] Art. 5, legge 15 dicembre 2001, n. 438, *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2001, n. 374, recante disposizioni urgenti per contrastare il terrorismo internazionale*, in *G.U.* n. 293 del 18 dicembre 2001.

[5] Decreto legge 27 luglio 2005, n. 144, *Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale*, in *G.U.* n. 177 del 1 agosto 2005.
Fortemente voluto dall'allora Ministro dell'Interno Pisanu a seguito degli attentati alla metropolitana di Londra del 7 Luglio 2005 e di Sharm el Sheik del 22 dello stesso mese, il decreto, tra le varie previsioni normative contenute, ha introdotto una serie di norme che facilitano le intercettazioni soprattutto da parte degli agenti dei servizi segreti, nonché con l'art. 6 sospese "*l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi*". Per completezza, occorre evidenziare che attualmente la norma di riferimento in questo delicatissimo settore è l'art. 132 del d.lgs. 196/2003, il c.d. "Codice della privacy", il quale prescrive al comma 1 che "*fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico, sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e*

Perché ciò potesse avvenire, invero, decisiva è stata l'esperienza maturata dal nostro legislatore nei decenni della lotta al terrorismo di Stato e alla criminalità organizzata, che ha permesso la creazione, già alcuni decenni fa, di strumenti giuridici particolarmente "flessibili", idonei oggi a far fronte anche alle nuove minacce terroristiche legate ad Al-Qaeda e ai gruppi ad essa collegati.

2. La protezione delle infrastrutture critiche nazionali dagli attacchi portati attraverso la rete Internet.

Da ultimo, una nuova minaccia alla sicurezza nazionale degli Stati pare acquisire sempre maggiore consistenza attraverso e per mezzo l'uso della rete Internet. All'incirca dal maggio 2006, infatti, un nuovo vocabolo è entrato prepotentemente nel registro linguistico degli analisti strategici e degli addetti alla sicurezza nazionale: *cyberwarfare*. Cercando di dare una definizione quanto più completa possibile del termine, al fine di spiegarne anche il fenomeno, per *cyberwarfare* si può intendere "la violazione non autorizzata da parte di, per conto di, oppure in sostegno a, un Governo nel computer di un altro Paese, nella sua rete o in qualsiasi altra attività interessata da un sistema informatico, al fine di aggiungere, modificare o falsificare i dati, ovvero causare l'interruzione o il danneggiamento, anche temporaneo, di uno o più computer, di uno o più dispositivi di rete, ovvero di qualsiasi altro oggetto controllato da un sistema informatico"[6]. Questo fenomeno[7], che attualmente interessa

---

repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione".

[6] Questa definizione non contempla al suo interno il concetto di "spionaggio elettronico", che è attività per molti versi completamente differente, almeno a livello teorico e di obiettivi, da quella di *cyberwarfare*.

[7] Occorre fare un'importante puntualizzazione: pur non potendo assolutamente negare l'esistenza di una concreta minaccia di *cyberwarfare* e dovendo anzi incoraggiare i Governi e le autorità militari a prendere in seria considerazione questo tema, contestualmente non si può sottacere l'esistenza di un problema semantico sul concetto, un po' abusato e distinto dal precedente, di *cyber-war*. Ad oggi, infatti, i *policymakers* faticano nel dare una precisa e giusta classificazione agli attacchi

maggiormente l'America[8], la Russia, la Cina ed alcuni altri Paesi dell'est, a causa dell'interconnessione mondiale della quasi totalità dei sistemi elettronici come pure della crescente dipendenza degli Stati occidentali da Internet e dagli strumenti tecnologici, negli ultimi due anni ha cominciato a preoccupare non poco anche i Paesi europei[9] e,

---

informatici, non riuscendo ad intuire dove e come allo stato attuale debbano essere inquadrati (come atti criminali, come atti di guerra ovvero come operazioni di spionaggio). Quello che è certo, però, è che gli attacchi informatici, effettuati sia fuori che dentro il cyber-spazio, possono essere diretta conseguenza di un più ampio disegno criminoso (atti criminali) e/o di un'attività di raccolta d'informazioni (operazioni di spionaggio), ma restano comunque e sempre meno pericolosi – a livello di minaccia – di un atto di guerra strettamente inteso.

La natura stessa del cyber-spazio, inoltre, ha la capacità (unica) di rendere praticamente uniformi gli squilibri politici che dominano le relazioni internazionali, ponendo sulla scacchiera i singoli individui, i piccoli e i grandi gruppi, così come gli Stati su un "piano di gioco" quasi paritario. In ogni atto di guerra, infatti, la fisicità di chi agisce – per mare, per terra, in aria o nello spazio – rende facilmente identificabili gli attori, così come facilmente individuabili sono anche i confini dello Stato belligerante. Lo stesso non avviene nel cyber-spazio, dove anzi, con un minimo di abilità tecnica, risulta veramente molto complesso non solo imputare l'azione ad uno o più determinati soggetti e/o ad uno Stato, quanto soprattutto evitare che chi ha realmente agito possa agevolmente manlevare se stesso da ogni responsabilità giuridica, politica, diplomatica, economica e militare.

Di conseguenza, allo stato dei fatti, potrebbe essere molto più conveniente parlare sempre di *cyberwarfare* o *cyber-conflicts* tra Stati piuttosto che di vere e proprie *cyber-war*, al fine di scongiurare ulteriori confusioni.

[8] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS), *Significant Cyber Incidents Since 2006*, CSIS, 2010.

Per approfondire lo studio sulla situazione americana, si veda S. MELE, *Le esigenze americane in tema di cyber-terrorismo e cyberwarfare. Analisi strategica delle contromisure*, in http://www.intuslegere.it/doc/cyber_warfare_s_mele.pdf, 2010.

[9] Numerosi Stati, europei e non, infatti, si sono già dotati di uno o più documenti ufficiali di *policy* per il settore della cyber-sicurezza. In ordine cronologico, si prendano in considerazione: MINISTRY OF DEFENCE OF ESTONIA, "*Cyber Security Strategy*", 2008, in http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf;

COMMISSION SUR LE LIVRE BLANC SUR LA DEFENSE ET LA SECURITE NATIONALE, "*Le Livre blanc sur la défense et la sécurité nationale*", 2008, in http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html; NATIONAL INFORMATION SECURITY POLICY COUNCIL, "*The Second National Strategy on Information Security. Aiming*

ovviamente, anche l'Italia[10]. Per questo motivo, creare le opportune capacità difensive idonee a far fronte a queste nuove minacce – reali o sovrastimate che siano – per la sicurezza delle infrastrutture critiche nazionali degli Stati è una delle nuove e più importanti priorità strategiche internazionali su cui porre al più presto l'attenzione, anche sotto l'aspetto normativo.

---

for Strong "Individual" and "Society" in IT Age", 2009, in http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf; SWEDISH EMERGENCY MANAGEMENT AGENCY, "*Information security in Sweden. Situational assessment 2009*", 2009, in http://www2.msb.se/Shopping/pdf//upload/Publikationsservice/MSB/0119_09_Information_security_in_Sweden.pdf; AUSTRALIAN GOVERNMENT, "*Cyber Security Strategy*", 2009, in http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity; U.S. GOVERNMENT, "*Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*", 2009, in http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ; CABINET OFFICE OF THE UNITED KINGDOM, "*Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space*", 2009, in http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf; COMMISSION OF THE EUROPEAN COMMUNITIES, "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*", 2009, in http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf; NATO PARLIAMENTARY ASSEMBLY, "*Committee Report 173 DSCFC 09 E bis - NATO and Cyber Defence*", 2009, in http://www.nato-pa.int/default.Asp?SHORTCUT=1782.

[10] L'Italia, attualmente, non si è ancora allineata agli Stati precedentemente menzionati, non producendo, almeno ufficialmente, un documento strategico specifico per questo settore. Ad ogni modo, da ultimo, in un recentissimo intervento pubblico presso la *Link Campus University* di Roma, il Direttore generale del DIS (Dipartimento delle Informazioni per la Sicurezza), Prefetto Giovanni De Gennaro, ha affermato che "*è ormai opinione condivisa che il principale campo di sfida per l'intelligence del terzo millennio sarà quello della cybersecurity; e sarà lì che si confronteranno gli organismi informativi delle Nazioni più sviluppate, nella piena consapevolezza della vulnerabilità dei rispettivi sistemi-paese, allorché il mondo del web avrà totalmente permeato costumi e modelli comportamentali dei loro cittadini, delle loro aziende, delle loro infrastrutture critiche, dei loro sistemi di comunicazione, dei loro assetti economici e finanziari. La* cyber-security *avrà allora la stessa valenza della difesa dal "nucleare" e forse anche di più, se si considerano i danni incalcolabili di un attacco informatico su larga scala*", sottolineando così l'attenzione che le nostre Istituzioni pongono sul tema.

3. La tecnologia a difesa della Rete.

Accertata la necessità e verificata la sua importanza, occorre comprendere (e forse anche accettare) che per creare un sistema di difesa realmente solido agli attacchi provenienti dalla Rete e aventi come obiettivo le infrastrutture governative, al di là di quali siano poi gli attori (Governi, terroristi e/o criminali), occorre essenzialmente monitorare il traffico Internet in transito in entrata e uscita sul territorio nazionale. Per far questo, occorre principalmente "mettersi in ascolto" sugli snodi principali di passaggio dei dati, chiamati *backbone*[11], ed effettuare in tempo reale un'analisi approfondita sul contenuto di ogni singolo pacchetto di dati[12] alla ricerca di quelli aventi un contenuto malevolo. Difendere questi nodi vitali della Rete significa proteggere tutte le infrastrutture critiche di uno Stato. E' proprio attraverso Internet, infatti, che le reti dei Governi, così come quelle delle società private, vengono costantemente poste sotto attacco ed è per questo che intercettare e individuare i vari tipi di attacchi già al loro ingresso sulle *backbone*, significa bloccare sul nascere qualsiasi intenzione criminosa e/o dannosa verso ogni rete bersaglio. Com'è facile immaginare, questo genere di controlli implicherebbe tre problemi principali: uno rigorosamente tecnico, l'altro di metodo organizzativo e l'ultimo normativo. Il primo, strettamente connesso ad un eventuale abbassamento delle *performance* di navigazione da parte degli utenti in caso di un'attività di analisi del traffico così invasiva; il secondo, riferito a "chi" e al "come" debba svolgere questo tipo di accertamenti e infine il terzo, apertamente legato al conflitto tra questo genere di sorveglianza elettronica e qualsivoglia norma giuridica posta a

[11] Sul mercato coesistono migliaia di *Internet Service Provider* (ISP) che offrono servizi di connettività e accesso alla Rete, ma, semplificando e banalizzando enormemente, solo pochi di essi (nell'arco delle poche decine) sono quelli che hanno la possibilità di raggiungere in maniera diretta e non mediata ogni altra rete presente su Internet e che, conseguentemente, "vedono" passare la quasi totalità del traffico telematico di loro competenza. In pratica sono gli ISP più vicini al "centro" di Internet e, pertanto, quasi il 90% del traffico mondiale passa per almeno una di queste *backbone*.

[12] Per una minima introduzione alla c.d. *deep packet inspection*, si prenda in considerazione la lettura di K. MOCHALSKI e H. SCHULZE, *Deep Packet Inspection. Technology, Applications & Net Neutrality*, in *Ipoque*, 2009.

salvaguardia della privacy e della protezione dei dati personali degli utenti, ovvero dei cittadini. Per far ciò, occorre individuare una metodologia organizzativa e tecnologica capace di analizzare il traffico nel modo meno invasivo possibile per l'utente, andando, successivamente, a valutare la sua (eventuale) "copertura" normativa. Muovendo il ragionamento nello specifico, a livello puramente tecnico, l'*hardware* e il *software* attualmente a disposizione aggirano con facilità il problema della perdita di *performance*, riuscendo ad analizzare ogni singolo *bit* di ogni pacchetto dati in transito senza per questo rendere misurabile la diminuzione della velocità di trasmissione delle informazioni (*no latency*) sui cavi in fibra ottica.

Anche la questione di metodo, legata principalmente alla scarsissima propensione di qualsiasi utente ad accettare che il Governo possa leggere il contenuto delle proprie e-mail e/o intercettare l'invio dei dati durante la navigazione Internet, può essere facilmente superata ancora una volta grazie all'intervento della tecnologia. Questa, infatti, è ormai capace di rendere la *deep packet inspection* non solo completamente automatizzata, quanto soprattutto legata non alla ricerca di determinate "parole chiave" (*keywords*), che potrebbero comportare la possibilità di spiare il contenuto delle informazioni trasmesse, ma all'individuazione delle "firme" (*signatures*) specifiche di ogni singolo attacco informatico[13].

A maggiore tutela dei cittadini, inoltre, questo compito potrebbe non essere affidato alla competenza del Governo, ma a quella dei *backbone Internet Service Providers (ISPs)*, che, ad ogni modo, già oggi possono "leggere" agevolmente la maggior parte del traffico Internet mondiale che transita in maniera non crittata per i propri

[13] Gli Stati Uniti d'America, attraverso il *Department of Homeland Security* (DHS) e lo *United States Computer Emergency Readiness Team* (US-CERT), dal 2004 hanno sviluppato e successivamente implementato un sistema molto simile di rilevamento delle intrusioni informatiche (*Intrusion Detection System o IDS*), denominato "EINSTEIN Program". Per i dettagli del progetto, si consulti U.S. DEPARTMENT OF HOMELAND SECURITY, *Privacy Impact Assessment for EINSTEIN 2*, in http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf , 2008.
Anche il *Department of Defence* (DoD) americano ha implementato un sistema simile a guardia dei 16 punti di accesso in cui la rete interna (*intranet*) non classificata si affaccia e si interconnette pubblicamente con la rete Internet.

sistemi[14]. Questo, naturalmente, implicherebbe la necessità di costruire sia un impianto normativo capace di assicurare una sorveglianza rigorosa sull'attività svolta a difesa del cyber-spazio da parte di questi *backbone Internet Service Providers* (*ISPs*), che uno specifico ufficio dedicato alla protezione e alla tutela delle libertà civili, magari incardinato all'interno del Garante per la protezione dei dati personali.

4. Le norme a difesa dei cittadini.

A questo punto occorre verificare se sia presente o meno nel nostro ordinamento giuridico la "copertura" legislativa per una simile attività di monitoraggio e controllo, ovvero, nei casi in cui non ci sia, se sia realmente opportuno crearla e in che termini. Tuttavia, ancor prima di fare ciò, si potrebbe anzitutto partire con il rendere sempre più vincolante l'art. 4 della Direttiva 2002/58/CE[15], irrigidendo così l'obbligo di notifica alle autorità, in caso di incursione nella sicurezza dei propri sistemi informatici, posto in capo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico[16]. A tal fine, si potrebbe prevedere un vero e proprio criterio di valutazione del rischio, ottenuto soppesando gli effetti negativi per gli utenti scaturenti da ogni singola violazione della sicurezza dei sistemi, in ragione, ad

[14] Ulteriori approfondimenti dovrebbero essere effettuati nel merito, soprattutto in relazione alla creazione e allo scambio sicuro delle "*signature*" degli attacchi tra i *backbone ISPs*, nonché ai ruoli di cui il Governo dovrebbe farsi carico affinché questi sistemi, ormai necessari, risultino sicuri e soprattutto accettabili per i cittadini. Tuttavia, esulando questi approfondimenti dal contenuto specifico di questo scritto, si è costretti a rimandare il ragionamento a future riflessioni.

[15] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, *relativa alla vita privata e alle comunicazioni elettroniche*, in *G.U.C.E.* n. L 201 del 31.7.2002, pagg. 37-47.

[16] Obbligo, inoltre, agevolmente estendibile anche a tutte le aziende che offrono quei servizi per la società dell'informazione maggiormente "sensibili" nell'ottica della protezione dei dati personali. Si pensi, ad esempio, ai sistemi che gestiscono le operazioni di Internet-*banking* o gli acquisti *on-line*, ovvero al problema emergente della c.d. privacy sanitaria e del fascicolo sanitario elettronico, per il cui approfondimento si rimanda a L. BOLOGNINI e G. FORGESCHI, *La next privacy nella sanità digitale italiana*, in *Next Privacy, il futuro dei nostri dati nell'era digitale*, RCS Etas, 2010.

esempio, della quantità di dati interessati dalla violazione (criterio quantitativo), della loro natura (criterio qualitativo), nonché delle dirette conseguenze per l'interessato, si pensi a un furto di identità, a un danno finanziario, a mancate opportunità economiche o occupazionali, ovvero ad una combinazione di questi fattori e/o di altre circostanze simili. La responsabilità di misurare il rischio per i dati personali degli utenti dovrebbe incombere, ovviamente, sui *backbone Internet Service Providers* (*ISPs*), essendo questi nella migliore posizione per stabilire, in tempi strettissimi e in base alle regole di valutazione stabilite dalle autorità preposte, quando e in che modo informare i soggetti interessati[17]. Dal momento che, però, la notifica

[17] In realtà questo principio è stato già previsto dal legislatore europeo che, da ultimo, attraverso la direttiva 2009/140/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in *G.U.C.E.* n. L 337 del 18.12.2009, pagg. 0037 – 0069, nota anche come "*Better Regulation Directive*", all'art 2, recante *Modifiche alla direttiva 2002/58/CE (Direttiva relativa allavita privata e alle comunicazioni elettroniche)*, apporta alcune rilevanti variazioni e integrazioni all'art. 4 della Direttiva 2002/58 in merito alla sicurezza del trattamento dei dati, prevedendo che "*in caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente.*
Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata.
[…]
Fatto salvo l'obbligo per i fornitori di informare gli abbonati e altri interessati, se il fornitore di servizi non ha provveduto a notificare all'abbonato o all'interessato la violazione dei dati personali, l'autorità nazionale competente, considerate le presumibili ripercussioni negative della violazione, può obbligare il fornitore in questionea farlo.
La comunicazione all'abbonato o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione all'autorità nazionale competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.
[…]
I fornitori tengono un inventario delle violazioni dei dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in misura sufficiente per consentire alle autorità nazionali

dovrà essere effettuata dal *backbone Internet Service Provider* (*ISP*), è essenziale allo scopo la creazione di una serie di norme e di principi che contemplino dei meccanismi sicuri volti ad evitare che le violazioni dei sistemi informatici vengano occultate, assicurando, inoltre, che la loro valutazione non avvenga in modo scorretto e che i soggetti interessati effettivamente ricevano le notifiche previste per legge[18].

Occorre evidenziare, comunque, che il Garante per la protezione dei dati personali ha più volte ribadito per il settore privato la regola generale che, tanto sul posto di lavoro[19] quanto nella vita privata[20], la

---

competenti di verificare il rispetto delle disposizioni di cui al paragrafo 3. Nell'inventario figurano unicamente le informazioni necessarie a tal fine".

[18] Nel merito, si prenda in considerazione anche quanto scritto in materia di notifica delle violazioni dei dati personali dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Parere 1/2009 sulle proposte recanti modifica della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, 10 febbraio 2009, in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_it.pdf

[19] L'art. 4 della legge 20 maggio 1970, n. 300 (il c.d. "Statuto dei lavoratori"), infatti, stabilisce che "*è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*". Inoltre, qualora gli impianti e le apparecchiature di controllo siano richiesti per far fronte ad esigenze organizzative e produttive ovvero di sicurezza sul lavoro, se dalla loro installazione ne deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori, il datore di lavoro è obbligato ad informare i dipendenti in modo particolareggiato e prendere opportuni accordi con i loro rappresentanti sindacali oppure, in mancanza, con la commissione interna (art. 4, comma 2, legge 300 del 1970). Pertanto, è consentita la vigilanza dell'impresa (c.d. controlli difensivi), ma non il controllo investigativo sull'attività dei lavoratori.
Medesimo ragionamento deve essere effettuato per i controlli del datore di lavoro sugli strumenti informatici in dotazione ai dipendenti (ad esclusione della casella di posta elettronica aziendale, che si ritiene essere strumento di lavoro e pertanto controllabile), ritenuti, tanto dalla giurisprudenza quanto dalla dottrina, controlli a distanza a tutti gli effetti e, quindi, ricompresi nel dettato dell'articolo 4 precedentemente richiamato. Anzi, per quanto attiene la navigazione su Internet, i sistemi informatici predisposti dal datore di lavoro devono essere configurati per cancellare periodicamente i dati personali relativi agli accessi ad Internet e al traffico telematico dei dipendenti, la cui conservazione non sia strettamente necessaria. Concetto ripreso anche dal Garante della Privacy con il *Divieto 2 aprile 2009 – Lavoro privato: monitoraggio degli accessi Internet del dipendente*, in cui si afferma

privacy degli utenti è un bene primario nell'attuale società dell'informazione e non può, pertanto, essere sottoposta ad attività di monitoraggio, registrazione e controllo.

Tra l'altro, sempre la Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, datata 12 luglio 2002, all'art. 5 ha da tempo affermato, come principio fondante, che gli Stati membri devono garantire, attraverso la loro legislazione nazionale, la riservatezza delle comunicazioni effettuate tramite una rete pubblica di comunicazioni elettroniche, proibendo, in particolare, ad ogni altro soggetto che non sia l'utente interessato di ascoltare, intercettare o memorizzare qualsiasi tipo di comunicazione non preventivamente ed esplicitamente autorizzata[21]. L'unica eccezione a questo assunto è data dal successivo

---

in maniera lapalissiana che "*è illecito monitorare in modo sistematico e continuativo la navigazione in Internet dei lavoratori*", violando questa condotta lo Statuto dei lavoratori.

[20] L'art.2, comma 1, del d.lgs. 30 giugno 2003, n. 196 (il c.d. "Codice della Privacy") afferma che il trattamento dei dati personali deve essere svolto "*nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*".

La Dichiarazione dei diritti umani, consultabile in italiano al seguente indirizzo http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=itn, all'art. 12, dispone che "*nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni*".

La Costituzione europea, invece, all'art II-68, si sofferma solo sulla obbligatorietà della protezione dei dati personali e, dopo aver affermato al primo comma che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*", successivamente prescrive che i dati debbano essere trattati "*secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge*". Il testo integrale della Costituzione europea è consultabile su: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2004:310:SOM:IT:HTML

[21] L'art. 5, paragrafo 1, della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, *Direttiva relativa alla vita privata e alle comunicazioni elettroniche*, letteralmente statuisce che "*gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza*

art. 15, paragrafo 1, in cui viene prescritto che gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi degli utenti nel solo caso in cui tale restrizione costituisca "*una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica*"[22], derogando così ai principi dell'anonimità e della cancellazione dei dati personali non più necessari[23]. E' evidente come un'interpretazione estensiva di questo articolo, affiancata da una prudente e stringente produzione normativa specifica, potrebbe portare ad ammettere a livello europeo la possibilità per gli Stati e per i *backbone Internet Service Providers* di effettuare attività di analisi approfondita dei pacchetti di dati in transito (*deep packet inspection*) alla ricerca delle *signature* degli attacchi.

Su una linea di pensiero più cauta si pone il legislatore italiano che, all'interno del Codice della privacy, ammette il trattamento dei dati personali, sensibili e giudiziari da parte delle forze di polizia[24], purché sia "*autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite*"[25] e

---

delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi".

[22] Art. 15, paragrafo 1, Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, *cit.*

[23] Deroga già prevista anche dall'art. 8, paragrafo 4, della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *Direttiva relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati*, in *G.U.* n. L 281/31, in cui l'utilizzo di informazioni concernenti la salute, la vita sessuale, la sfera religiosa, politico-sindacale o filosofica, nonché l'origine razziale ed etnica degli utenti deve essere soggetto a rigorose cautele, in base alle quali è vietato il loro trattamento a meno che non ricorrano "*specifici motivi di interesse pubblico rilevante e siano altresì assicurate opportune garanzie*".

[24] Art. 53, comma 1, d.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, in http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248

[25] Art. 20, comma 1, d.lgs. 30 giugno 2003, n. 196, *cit.*

sempre che ne sia precedentemente verificata la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto agli obiettivi perseguiti nei singoli casi[26], soprattutto nell'ipotesi in cui la raccolta dei dati non avvenga presso l'interessato. Cautele molto simili a quelle appena richiamate sono previste, poi, per il trattamento dei dati effettuato da soggetti pubblici per finalità di difesa o di sicurezza dello Stato[27], per il quale, in ragione della "delicatezza" dei compiti assegnati, si applicano però solo una piccola parte delle disposizioni del Codice[28].

Dall'analisi appena svolta, è fuor di dubbio come allo stato attuale manchi un vero e proprio substrato normativo solido – sia a livello europeo che nazionale – capace di accogliere la possibilità di concedere ad un soggetto privato (come un *backbone Internet Service Provider*) l'onere di sorvegliare gli snodi principali della rete Internet alla ricerca delle *signature* degli attacchi informatici e, per l'effetto, di difendere i sistemi elettronici delle infrastrutture critiche nazionali. Eventualità, invece, che potrebbe essere riconosciuta più agevolmente, con giuste e ulteriori cautele normative, ai soggetti giuridici statali che si occupano di salvaguardare la sicurezza e la difesa dello Stato.

5. Conclusioni.

L'utilizzo della tecnologia di *deep packet inspection*, soprattutto così come definita e "compressa" fino ad ora, non appare di per sé né lecita e neppure illegale. Risulta tale in dipendenza del soggetto che la

[26] Art. 22, comma 5, d.lgs. 30 giugno 2003, n. 196, *cit.*
Completa il quadro normativo l'art. 54, comma 3, che demanda al Centro elaborazioni dati delle forze di polizia "*l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati*".
[27] Art. 58, d.lgs. 30 giugno 2003, n. 196, *cit.*
[28] L'art. 58, comma 1, infatti, afferma che "*ai trattamenti effettuati dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge, le disposizioni del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169*", "*nonché alle disposizioni di cui agli articoli 37, 38 e 163*", così come previsto dal comma 2 del medesimo articolo.

usa, dei modi in cui viene adoperata e a seconda degli scopi per cui viene impiegata. Da quanto detto e dall'analisi della legislazione nazionale ed europea, emerge in maniera chiara che alcuni principi devono essere considerati fondamentali quando ci si vuole accostare ad un uso lecito e trasparente della *deep packet inspection*, nonostante, lo si ribadisce, la tecnologia al momento offra la possibilità di ricercare nei pacchetti dati in transito non delle parole specifiche (*keywords*), ma delle semplici *signature*. In particolare, questi principi sono:

- operare con trasparenza, affinché gli Stati o gli *ISPs* che si accingono a svolgere questo genere di attività si preoccupino di fornire agli utenti tutte le informazioni necessarie sui metodi di raccolta, analisi, uso e cancellazione dei dati personali;
- Coinvolgere gli utenti, al fine di ottenere, per quanto possibile, il loro consenso individuale alla raccolta, all'analisi e all'uso dei dati;
- specificare le finalità, in modo da chiarire e inquadrare gli obiettivi per cui si adotta questo genere di tecnologia, onde evitare eventuali attività arbitrarie;
- ridurre al minimo i dati, non ovviamente nella fase di raccolta, nella quale tutti i pacchetti in transito possono essere potenziali attacchi e devono pertanto essere captati, ma di sicuro nella fase di analisi e uso degli stessi, garantendo così che solo quelli le cui firme (*signature*) siano corrispondenti a quelle presenti nel database del *backbone Internet Service Provider* siano realmente presi in considerazione e utilizzati;
- limitare l'uso, garantendo così che la tecnologia di *deep packet inspection* possa essere utilizzata esclusivamente per le finalità specificate;
- implementare alti livelli di sicurezza, al fine di proteggere in maniera più che adeguata tutti i sistemi deputati a queste attività contro i rischi di accesso abusivo, perdita, uso scorretto, distruzione intenzionale, modifica o divulgazione inappropriata dei dati degli utenti;
- *accountability* e *auditing*, attraverso i quali i *backbone Internet Service Providers* devono essere responsabili della concreta attuazione e del rispetto dei principi finora richiamati, nonché della

conformità dei loro sistemi ad essi e a tutti gli ulteriori requisiti in materia di sicurezza e privacy previsti dalla legge.

Soltanto attraverso questi "passi" si può giungere all'obiettivo finale di rendere accettabile questo genere di attività che, oggigiorno, pare essere ormai indispensabile per far fronte alle minacce di *cyberwarfare*, ma anche per garantire ai cittadini una giusta protezione dai continui attacchi da parte di criminali sempre più preparati tecnicamente e con sempre meno scrupoli, consapevoli di agire in Rete con un'altissima probabilità di anonimato e, pertanto, anche di impunità.

Il trattamento dei dati personali nell'analisi del comportamento del consumatore

di Giovanni Crea [(*)]

SOMMARIO: 1. Introduzione. – 2. Dalla produzione di massa alla mass customization. – 3. Sulla natura personale della funzione di utilità del consumatore. – 4. Stima della funzione di utilità del consumatore e implicazioni sulla riservatezza. – 5. Sulla circolazione dei dati personali nella società dell'informazione. – 6. Conclusioni.

1. Introduzione.

La letteratura, prevalentemente giuridica, sul trattamento dei dati personali appare pressoché compatta nel sostenere una linea di protezione che, anche in campo economico, sia garantista dei consumatori in misura tale da subordinare alla loro esplicita e libera autorizzazione qualunque operazione dell'impresa che possa eccedere quelle minime necessarie per il concreto svolgimento del rapporto di scambio. D'altro canto, l'opportunità per l'economia e per gli stessi consumatori di un trattamento dei dati personali finalizzato alla conoscenza delle loro abitudini di consumo e delle funzioni di soddisfazione – o, per usare un termine tecnico, delle funzioni di *utilità* – trapela indirettamente dalla letteratura economica, in particolare da quella che si occupa dell'analisi del comportamento del consumatore, ma anche dai contributi che trattano di quella fase del cambiamento che sta permeando l'economia e le società in cui l'informazione ha assunto i connotati di una vera e propria risorsa produttiva e il suo trattamento è diventato parte del processo produttivo. Fortemente interessato a dati del singolo consumatore, riguardanti il suo comportamento sul mercato, è senza dubbio il settore distributivo (*retailing*); per le imprese ivi operanti la

[(*)] Università Europea di Roma; Istituto Italiano per la Privacy.

segmentazione dei consumatori appare un passaggio irrinunciabile per cogliere le cause che stanno dietro le differenze di comportamento e porre in essere politiche commerciali anch'esse differenziate. Le *Information and communication technologies*[1] (Ict), con le applicazioni *off line*, le reti e i servizi di comunicazione elettronica e i *software* di ricostruzione dei profili individuali, hanno finito per identificarsi con forme sofisticate di trattamento come la localizzazione e il *profiling*. Grazie a queste tecnologie, ad esempio, una compagnia di assicurazioni che opera in condizioni concorrenziali potrebbe monitorare il comportamento di guida dei propri clienti e concedere sconti sul premio assicurativo (o altre agevolazioni), in aggiunta al classico *bonus*, nel caso di condotta prudente[2]. Per le imprese *e-commerce*, ma anche per quelle che hanno spostato solo in parte la loro attività in Internet, le Ict rappresentano un'opportunità senza precedenti per disporre di un profilo pressoché completo del *cyber*-consumatore. La prospettiva della società dell'informazione ha fornito l'occasione – almeno alla schiera dei sostenitori del libero mercato – per tornare sul *trade off* associato ai dati personali, ossia sulla condizione in cui si confrontano il diritto al trattamento, inteso come un aspetto della libertà di iniziativa economica, e quello alla riservatezza. Al riguardo, merita precisare come nel dibattito non siano in discussione i principi della necessità, della trasparenza e della proporzionalità, a cui il trattamento deve conformarsi, quanto la regola del suo avvio; in un'ottica di equilibrio dei predetti diritti, si discute cioè se appare giustificato subordinare il trattamento a un'esplicita approvazione dell'interessato, senza che ciò possa costituire un'eccessiva compressione della libertà d'impresa, o se, al contrario, il trattamento potrebbe essere svolto liberamente, assumendo che

[1] Si tratta di tecnologie di trattamento dell'informazione che ricomprendono anche la funzione della trasmissione (*communication*).

[2] L'esempio è tratto dal saggio di J. ROSENBERG, *Google: i sistemi "aperti" sono vincenti*, in *Consumatori, Diritti e Mercato*, n. 1, 2010, 56-63. Oltre le tecnologie satellitari, il controllo del comportamento di utenti e consumatori può essere attuato attraverso dispositivi di identificazione che sfruttano le frequenze aeree (Rfid); al riguardo v. A. MANTELERO, *Identificatori a radiofrequenza (RFID) e controllo capillare dei dati personali: il rischio di un «mondo nuovo» per il consumatore?*, in *Contratto e impresa / Europa*, n. 1, 2004, 1-16.

l'assenza di un pronunciamento abbia il significato di consenso, ben inteso sempre che l'interessato sia posto nelle condizioni di opporsi, in tutto o in parte e in qualsiasi momento, all'uso dei dati che lo riguardano. Sul piano del diritto, la disputa *opt-in vs. opt-out* – che pone di fronte un regime che esalta il primato dei diritti fondamentali della persona e uno più vicino alla visione liberista – ha conosciuto alterne vicende che hanno visto prevalere l'opzione positiva[3], se pure recentemente l'opzione negativa ha registrato un punto a favore nel diritto interno; detta opzione – vale ricordarlo – è stata introdotta alla fine del 2009 con riguardo al trattamento consistente nella raccolta di numeri telefonici e dei corrispondenti nominativi, nell'organizzazione di tali dati in opportuni archivi e nel loro uso attraverso il servizio di comunicazione telefonica interattiva[4] per scopi di commercializzazione diretta. Al di là delle considerazioni a sostegno dell'una o dell'altra opzione, nota dolente delle Ict è che esse hanno introdotto *software* idonei ad attuare un trattamento occulto dei dati personali contribuendo all'aumento dei casi di violazione della normativa; in particolare, il *digital profiling* quasi mai risulta conforme alla disciplina preposta alla protezione dei dati personali, il che evidenzia la debolezza di quest'ultima in termini di *enforcement*. Al riguardo, rileva sottolineare come un simile trattamento sia spesso svolto all'insaputa degli interessati che dunque non possono esercitare, neppure successivamente al suo avvio, i diritti nei quali si riassume l'autodeterminazione sulle proprie informazioni[5]; ed è quasi

[3] Per una ricognizione giuridica più approfondita si veda M. A. SENOR, *Comunicazioni indesiderate: tecniche commerciali, spamming e consenso dell'interessato*, Atti del convegno *"I diversi aspetti del diritto alla protezione dei dati personali"*, Torino, 10 giugno 2004.

[4] Il carattere interattivo della comunicazione telefonica è rilevante ai fini dell'applicazione della regola negativa. Al riguardo, vale ricordare che lo stesso trattamento è sottoposto al regime *opt-in* nel caso in cui i numeri telefonici sono utilizzati attraverso il servizio telefonico automatizzato, senza cioè l'intervento di un operatore. Cfr. Direttiva 2002/58/CE, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, in *GUCE*, L 201, del 31 luglio 2002, articolo 13, paragrafo 3.

[5] La questione può essere riguardata come un particolare aspetto del più generale problema della regolazione di Internet per i cui approfondimenti si rimanda alla

superfluo ricordare come una simile condotta sia contraria al principio della trasparenza, stabilito dalla disciplina comunitaria e a cui i responsabili del trattamento dovrebbero conformarsi. Questo lato offuscato del trattamento tecnologico riguarda sia le applicazioni «esterne» alla Rete sia le attività «interne» alla stessa; e, specie per Internet, va detto che i *provider* che attuano in modo invisibile il *digital profiling* sono anche quelli dominanti, la cui posizione di mercato riposa sulla possibilità di effettuare questo trattamento. Tale modalità – una volta intuita – è però suscettibile di determinare una perdita di fiducia degli utilizzatori nei confronti della Rete; esito, questo, che non è certo esente da rischi di ricadute (negative) sul commercio elettronico, in particolare sotto il profilo della sicurezza delle transazioni *on line*, posto che queste implicano uno scambio di dati personali[6].

D'altro canto, il trattamento in Rete, consistente nella determinazione di profili individuali, è un'operazione necessaria per lo sviluppo dell'economia della società dell'informazione; per di più, detta operazione va inquadrata in un contesto dinamico alla luce dei possibili mutamenti, nel tempo, della scala delle preferenze del consumatore. In questa prospettiva, la c.d. 'profilazione' svolta in conformità al principio della trasparenza andrebbe interpretata in chiave di opportunità di mercato piuttosto che alla stregua di un'incombenza normativa; e, invero, l'informativa ai consumatori sul trattamento dei dati che li riguardano può essere considerata un aspetto di quell'approccio relazionale delle imprese, nato dall'esigenza di adeguarsi ai cambiamenti imposti dalla disgregazione della domanda e dei mercati, attraverso il quale esse possono conquistare la fedeltà dei consumatori. In una fase dell'economia in cui i dati riguardanti le caratteristiche dei *singoli* consumatori sono essenziali per progettare prodotti e servizi commisurati alle loro

letteratura in materia quale A. MANTELERO, *regole tecniche e regole giuridiche: interazioni e sinergie nella disciplina di internet*, in *Contratto e impresa*, n. 2, 2005, 658-686, e, volendo, G. CREA, *La neutralità della rete, tra concorrenza, società dell'informazione e libertà di espressione*, in *Quaderni di Diritto ed economia delle comunicazioni e dei media*, Roma, Aracne, 2008, 49-84.

[6] Sul punto, cfr. P. GUARDA, *Sicurezza dei pagamenti e privacy nell'e-commerce*, in *Diritto dell'Internet*, n. 1, 2005, 91-101.

utilità, i paradigmi che devono guidare il rapporto tra offerta e domanda non possono essere più quelli che, un tempo, riflettevano il primato dell'impresa. Tutto è iniziato con il passaggio dall'economia di massa all'economia di varietà, che ha imposto alle imprese una frammentazione dell'offerta; transizione non indolore sia sotto il profilo dell'efficienza – il fabbricante non può più contare sull'omogeneità del prodotto e sulle economie di scala, ma deve ricorrere a nuove forme di efficienza, in particolare all'adozione di sistemi di produzione in grado di realizzare *output* variabili[7] – sia per la necessità di accesso ai dati personali che però non è scontato in ragione dei vincoli posti dal diritto alla riservatezza. A dirla tutta, va precisato che, già in pieno fordismo, le imprese avevano colto segnali di mutabilità della domanda e avviato alcuni adeguamenti del processo produttivo che lo potessero rendere più flessibile[8]; il paradigma fordista – forte delle sue economie di scala – non ha tuttavia facilitato il passaggio a una *lean production* spinta sotto il profilo della variazione del prodotto. Bisogna attendere oltre la metà del Novecento per l'avvento dell'economia di varietà; da quel periodo

[7] Le economie di varietà (o economie di scopo) si realizzano se il costo della produzione di più beni ottenuta con i medesimi fattori produttivi è inferiore alla somma dei costi sostenuti per la produzione separata (impiegando fattori distinti) di ciascuno dei beni. Nel caso esemplificativo di due beni, di cui si producono le quantità *x* e *y* rispettivamente, le economie di varietà si conseguono se si verifica la disuguaglianza $C(x, y) < C(x, 0)+C(0, y)$.

[8] I primi segnali di cambiamento si iniziano a intravedere in seguito alla crisi del 1929 e con l'ingresso sui mercati di nuove imprese. Quest'ultima circostanza diminuì la capacità delle imprese di realizzare le economie di scala – fattore critico del paradigma fordista – e spinse le stesse ad adeguare il proprio processo produttivo alle prime forme di diversificazione, passando dalle economie di scala a quelle di varietà. La messa in esistenza di linee di produzione distinte, i cui prodotti, pur avendo la medesima funzione d'uso, erano adattati alle caratteristiche di gruppi diversi di consumatori, ha rappresentato il primo passo di allontanamento dalla produzione omogenea nella direzione di quella differenziata. Per un approfondimento sulla transizione dall'economia di massa all'economia di varietà v. R. GRANDINETTI, *Il rapporto tra produzione e consumo in una prospettiva storica*, in R. GRANDINETTI (a cura di) *Marketing. Mercati, prodotti e relazioni*, Roma, Carocci, 2008; G. COZZI, B. DI BERNARDO, E. RULLANI, *Marketing e tecnologie dell'informazione: dall'economia di massa all'economia della varietà*, in *Scritti in onore di Luigi Guatri*, Milano, ed. Bocconi Comunicazione, 1988.

inizia un processo di diversificazione dell'offerta che oggi tenta di interpretare perfino ciò che in tempi ormai risalenti la psicologia aveva posto all'attenzione degli economisti, vale a dire la natura soggettiva – dunque personale – del comportamento del consumatore, che lo rende ben diverso da quello ideale (*homo oeconomicus*) rappresentato dalla teoria economica[9]; il che equivale a dire che i consumatori hanno una funzione di preferenza/utilità propria, psicologica e dinamica, che ha poco a che fare con il modello curvilineo offerto dalla teoria economica.

Sotto questo aspetto, merita sottolineare come la differenziazione personale dell'offerta abbia superato i confini del bene per concentrarsi su elementi di «rivestimento» immateriale (si pensi all'*atmosfera* del luogo di vendita ovvero alle caratteristiche *esperienziali* incluse nell'offerta di un prodotto turistico). Strategia, questa, che riposa su dati di comportamento che racchiudono anche caratteristiche soggettive che operano una qualche mediazione degli stimoli esterni. È pacifico, pertanto, concludere sulla necessità delle informazioni personali per la ricostruzione – sia pure imperfetta – delle preferenze dei consumatori e per seguirne i mutamenti nel tempo e nello spazio; anche alla luce della disciplina in materia di protezione dei dati personali, la chiave di accesso a tali risorse va ricercata nel rapporto che le imprese instaurano con i consumatori, in particolare nella capacità di infondere in questi ultimi uno stato di fiducia.

Il lavoro propone alcune riflessioni sul ruolo che il trattamento dei dati personali assume nell'analisi del comportamento del consumatore. Questo filone dell'analisi economica ha messo in luce, sia pure indirettamente, la necessità, per le imprese, della conoscenza della funzione di utilità reale del consumatore su cui costruire l'offerta; informazione, questa, che ha natura personale e che è

[9] Le origini dello studio del comportamento del consumatore possono essere fatte risalire al pensiero di Gabriel Tarde che, nel 1881, intuì l'opportunità di avvicinare la prospettiva economica e quella psicologica. Non va peraltro dimenticata la più concreta iniziativa di George Katona che, nel 1975, con la sua opera *Psychological economics*, sancì definitivamente il connubio tra psicologia e teoria economica, esaltando il contributo della prima alla spiegazione del comportamento degli agenti economici. Al riguardo, cfr. G. TARDE, *La psychologie Economique*, 2 voll., Paris, Alcan, 1902; G. KATONA, *Psychological economics*, New York, 1975.

derivata dall'elaborazione di dati personali elementari. La disciplina giuridica del trattamento dei dati personali impone alle imprese una modalità di reperimento dei dati sottostanti che non sia 'predatoria', ma che possa svolgersi all'insegna della trasparenza e della libera decisione degli interessati. Peraltro, i vincoli di mercato (la concorrenza, i mutamenti della domanda, le prospettive di accesso a nuovi mercati) suggeriscono alle imprese di ricondurre la questione dell'accesso ai dati personali nell'ambito di un rapporto di simbiosi con la domanda individuale, in cui quest'ultima possa rilasciare, secondo le sue esigenze, informazioni sulle proprie preferenze.

Sul fronte delle politiche comunitarie, rileva osservare come le iniziative messe in campo per il passaggio alla società dell'informazione non possano prescindere dalla circolazione transfrontaliera di dati personali, e dunque anche dall'accesso ai medesimi, essendo tale condizione funzionale alla realizzazione del mercato unico e alla crescita dell'economia dell'Unione europea. L'apertura che il modello della società dell'informazione sembra prospettare alle imprese va tuttavia interpretata alla luce del quadro normativo sul trattamento dei dati personali, imperniato sulla regola del libero ed esplicito consenso da parte dei consumatori (e, più in generale, degli interessati); la limitazione alla diffusione dei dati personali che questa regola opera è il prezzo che l'economia paga per ridurre i rischi di violazione della sfera personale che, specie nel caso della navigazione in Internet, i consumatori corrono.

Nella prospettiva della società dell'informazione, i diritti dei consumatori e quelli delle imprese si incontrano sul terreno dell'Ict; ed è probabilmente in tale contesto che va ridisegnato il loro equilibrio, ribaltando la deriva che le tecnologie hanno assunto, da strumento di violazione del diritto a braccio operativo del medesimo. Sotto questo aspetto, ad esempio, si può immaginare che, grazie alle Ict, i consumatori possano decidere se e in che misura consentire il *profiling* in tutte le occasioni – *on line* e *off line* – in cui essi entrano in contatto 'tecnologico' con le imprese.

2. Dalla produzione di massa alla mass customization.

La rilevanza dei dati personali in economia è ben nota; senza tali risorse la comprensione dei fenomeni comportamentali della domanda sarebbe rimasta confinata ai modelli della teoria economica neoclassica. Per lungo tempo, l'impronta *normativa* di questi modelli ha condizionato l'interpretazione del comportamento del consumatore costringendola entro il perimetro di alcune intuizioni e di assiomi non verificati nella realtà[10]. È stata probabilmente la visione *positiva* di alcuni economisti (Mill, Thaler, Friedman), con l'ammissione della valenza approssimativa di tali modelli, a dischiudere alla prospettiva di un approccio empirico all'analisi della domanda; approccio che ha fatto comprendere anche agli economisti l'opportunità di disporre di dati di carattere personale da cui poter ricostruire profili anch'essi personali. Peraltro, al di là delle vedute più o meno realistiche della scienza economica, in tempi risalenti l'accesso a dati sulle abitudini dei consumatori non era, tutto sommato, una condizione imprescindibile dell'impresa per la conquista di quote di mercato. I dati personali erano sottoposti a trattamenti minimi, necessari a svolgere il rapporto di scambio; nell'ambito della fornitura dei servizi di pubblica utilità, ad esempio, i dati di consumo dei singoli utenti, dopo essere stati utilizzati per ricevere il corrispondente valore monetario, venivano aggregati – in tal modo si perdeva il contenuto personale – e impiegati nelle analisi di traffico finalizzate al dimensionamento delle reti. Un simile atteggiamento delle imprese va interpretato alla luce dello stato di avanzamento tecnologico e della fase economica del periodo, che possiamo inquadrare tra la fine dell'Ottocento e gli anni 50-60 del secolo scorso. Sul punto rileva osservare che le tecnologie di quei tempi non consentivano trattamenti su elevati volumi di dati, come l'immagazzinamento, se non a costi

[10] È noto che la razionalità del comportamento del consumatore è ben diversa da quella rappresentata dalla teoria dell'utilità; questa descrive il consumatore come un sistema cognitivo, le cui regole di valutazione dell'utilità delle alternative di scelta coincidono con un modello matematico. I consumatori sono sistemi cognitivi autonomi che tendono a ottimizzare le proprie funzioni di utilità seguendo procedure meno teoriche, euristiche, senza che per questo possa dirsi che un tale comportamento sia irrazionale.

elevati. A ciò si aggiunga che, al di là dei problemi di capacità dei sistemi informativi, l'economia era caratterizzata dal primato della produzione, che dunque guidava il consumo[11]. Le strutture monopolistiche o, al più, oligopolistiche, dei mercati dell'epoca non ponevano alle imprese protagoniste problemi di reperimento di dati di natura personale che potessero fornire indicazioni sulle diverse preferenze della domanda; e – a dirla tutta – fino alla ricostruzione industriale neppure la domanda mostrava differenze di comportamento sul mercato in misura tale da giustificare una *varietà* della produzione che potesse essere destinata a segmenti più ristretti[12]. Era il tempo dell'economia fordista-taylorista in cui prevalevano la produzione omogenea e il consumo di massa; grazie alle economie di scala, un siffatto modo di produzione consentiva alle imprese di praticare prezzi accessibili e di far crescere la domanda che dunque poteva realizzare quei bisogni di appartenenza sociale, di conformismo, descritti in letteratura come effetto *bandwagon*[13]. L'esigenza di uniformità che si manifestava anche dal lato del consumo lascia facilmente comprendere come un rapporto di tipo *broadcasting* tra offerta e domanda sia stato più che sufficiente a soddisfare bisogni generalizzati. Secondo una diversa lettura del fenomeno, in quel periodo l'assenza di ricerca di varietà dal lato della domanda era spiegata da una sorta di compromesso tra produzione e consumo in virtù del quale i consumatori avrebbero rinunciato a manifestare preferenze "troppo particolari" per accedere a beni inizialmente riservati a fasce ristrette della popolazione[14]. Pochi problemi, dunque, di contemperamento tra il diritto dell'impresa

[11] Cfr. G. COZZI, S. VACCÀ, *Consumo e tecnologia nel capitalismo contemporaneo*, in *Il Ponte*, vol. 45, n. 1, 1989, 45-71.

[12] Sul punto sia consentito il rinvio a G. CREA, *La protezione dei dati personali tra diritti d'impresa, dei consumatori e della concorrenza*, in L. BOLOGNINI, D. FULCO, P. PAGANINI (a cura di), *Next privacy. Il futuro dei nostri dati nell'era digitale*, Milano, Etas, 2010, 138-190.

[13] Cfr. H. LEIBENSTEIN, *Bandwagon, Snob and Veblen Effects in the Theory of Consumers' Demand*, in
The Quarterly Journal of Economics, n. 64, 1950.

[14] Sul punto, S. BARBIERI, R. FIOCCA, *Dal broadcasting al narrowcasting: effetti su imprese, consumatori e agenzie di pubblicità*, in *Economia & Management*, n. 1, 1996, 32.

all'iniziativa economica e il diritto alla riservatezza di tutto ciò che era considerato personale e che tale iniziativa poteva toccare (gusti, consumi e altre caratteristiche dei consumatori). Ma nulla è per sempre. A partire dalla fase più matura della società industriale, si assiste all'emersione di motivazioni nei consumatori di natura diversa dai bisogni primari e di ordine pratico. Il consumo è divenuto un fenomeno più complesso che non ha mancato di attirare l'interesse di numerosi studiosi che hanno proposto modelli interpretativi delle motivazioni sotto il profilo evoluzionistico[15]. In altre parole, la domanda ha finito per emanciparsi dalla produzione manifestando la sua natura multidimensionale e dinamica, stimolata anche dall'evoluzione tecnologica. Con riguardo a quest'ultimo aspetto, rileva osservare che le tecnologie ad ampio spettro di applicazione (*general purpose technologies*)[16], che sono state alla base della macchina a vapore, dell'elettricità, delle telecomunicazioni di prima generazione, hanno determinato nuovi bisogni nei consumatori nei confronti di servizi che hanno finito per essere di pubblica utilità. In tempi più recenti, le *information technologies*, con i metodi di rappresentazione binaria dei dati (ossia di conversione dei contenuti in successioni di 0 e 1), e i connessi sviluppi sul fronte delle *communication technologies*, hanno posto le basi per la transizione verso un'economia orientata a bisogni di conoscenza, partecipazione, appartenenza, espressione, ai quali va ricondotto l'uso di Internet. E non solo. Nel frattempo, l'incremento della produttività, le conquiste sindacali, l'aumento del benessere, hanno determinato l'ampliamento del tempo extralavorativo disponibile in cui hanno preso forma bisogni per lo più di natura edonistica (desideri), per il soddisfacimento dei quali gli individui e le imprese si sono incontrati su nuovi mercati. L'economia derivata da questi mutamenti è l'economia del tempo libero in cui i beni scambiati (*leisure goods*)

[15] Per tutti, si veda A. MASLOW, *Motivation and personality*, New York, Harper and Brothers, 1954.

[16] Sulle *General purpose technologies* (*GPTs*) cfr. R. G. LIPSEY, K. I. CARLAW, C. T. BEKAR, *Economic trasformations. General purpose technologies and long-term economic growth*, Oxford e New York, 2005. Si veda anche il più recente saggio di D. FREDDI, *Technology extension policies: caratteristiche, finalità e contesti applicative*, in *Economia e politica industriale*, n. 1, 2009.

sono rappresentati dall'intrattenimento, da eventi e rappresentazioni con contenuto esperienziale e da prestazioni atte a determinare negli individui una trasformazione voluta e durevole[17].

Dal lato delle imprese, le implicazioni della disgregazione della domanda sono intuibili anche alla luce della crescente pressione concorrenziale; i processi interni – produttivi, distributivi, organizzativi – si sono modificati in un'ottica di *mass customization* (varietà del prodotto a costi decrescenti), in altre parole, cercando una maggiore flessibilità[18] per diversificare l'offerta e destinarla a gruppi sempre più ristretti di consumatori in una prospettiva di efficienza (economie di varietà). Ma in un contesto in cui la domanda è suscettibile di continue variazioni e in cui, per tale ragione, il tempo è una variabile concorrenziale decisiva (*time based competition*), occorre anche che le imprese siano capaci di minimizzare i periodi di adattamento dei processi interni[19]. Di qui, l'esigenza di disporre di

[17] L'offerta di intrattenimento ha assunto nuovi profili che vanno oltre quelli tradizionali i cui contenuti sono fruibili direttamente nei luoghi di rappresentazione (teatri, sale cinematografiche, stadi, locali notturni) o attraverso i mezzi di comunicazione. L'intrattenimento si è esteso anche a settori commerciali diversi sotto il profilo merceologico – si pensi alla ristorazione e all'abbigliamento – in cui esso svolge un ruolo complementare, di 'rivestimento' dell'offerta specifica di quei settori. L'economia delle esperienze descrive un particolare profilo dell'economia del tempo libero in cui i beni scambiati integrano quasi totalmente contenuti memorabili, meno transitori, che cioè restano impressi nei fruitori per un tempo più ampio rispetto a quello in cui si mantiene il ricordo di un contenuto di intrattenimento. Il settore del turismo è un esempio di ambito economico in cui l'esperienza è parte del bene oggetto di offerta. Tra i beni che, invece, caratterizzano la c.d. economia delle trasformazioni si possono elencare il *fitness*, il *wellness*, le discipline artistiche, i corsi specialistici.

[18] Cfr. M. E. GARBELLI, *Over-Supply and Manufacturing Localization*, in *Simphonya. Emerging Issues in Management*, n. 1, 2002.

[19] L'argomento si inquadra nel più generale concetto di adattamento dell'impresa ai condizionamenti provenienti dall'ambiente di riferimento. Sotto questo profilo, la capacità dell'impresa si misura sia nelle modalità con cui questa si relaziona con l'ambiente esterno (consumatori, organizzazioni, istituzioni, …) sia nei tempi in cui effettua gli interventi di adeguamento dei processi interni. Sul punto, cfr. G. DEL CHIAPPA, *La time based competitive knowledge nello sviluppo di nuovi prodotti: la dimensione interna e interorganizzativa*, in *Economia e Diritto del terziario*, n. 1, 2004. Sulla *time based competition*, v. anche S. M. BRONDONI, *Economie d'impresa globale e dinamiche competitive*, in *Symphonya. Emerging Issues in Management*, n.

informazioni che riguardano il consumatore e che possono spiegare il suo comportamento sul mercato; questione non di poco conto, se si considera che queste informazioni colgono profili specifici del consumatore (abitudini di acquisto e consumo, preferenze, livelli di spesa) che si inquadrano nella sua sfera personale[20], e il cui trattamento è suscettibile di violarne la riservatezza, essendo questa uno dei diritti fondamentali della persona. Vale la pena accennare come anche la percezione della dimensione privata si sia trasformata con l'evoluzione tecnologica e i connessi mutamenti sociali; l'ambito personale non è più identificabile come tutto ciò che resta all'interno dei confini domestici, ma è un insieme di contenuti che è tale ovunque, e ovunque ne va garantita la privacy[21]. A ben vedere, senza attendere l'era digitale, l'accezione *a-dimensionale* della sfera personale e del diritto alla sua riservatezza si intuisce già dalla vicenda di fine Ottocento dell'avvocato S. Warren che vide le sue abitudini mondane messe di proposito in piazza dalla stampa americana; vicenda che indusse l'interessato, con il sostegno dell'amico di studi L. Brandeis, a rivendicare con successo, nel 1890, il *right to be let alone*[22] (oggi, con l'Ict e Internet, le informazioni su quelle abitudini sarebbero state trasformate in elementi digitali e offerte alla curiosità di un pubblico ben più ampio degli abitanti di Boston).

L'economia riposa dunque sulla disponibilità di informazioni che danno conto dei comportamenti individuali; come a dire che ogni

---

1, 2005; S. H. HUM, H. H. SIM, *Time-Based Competition: Literature Review and Implications for Modelling*, in *International Journal of Operations & Production Management*, vol. 16, n. 1, 1996, 75-90.

[20] In tal senso, cfr. V. GRIPPO, *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in *Riv. crit. dir. priv.*, 1998.

[21] In questa prospettiva, anche la privacy, ossia la condizione in cui la sfera personale è sottratta all'altrui conoscenza, è stata riconosciuta come un interesse la cui tutela è indipendente dai luoghi. Al riguardo, cfr. decisione *Katz v. United States*, 389 U.S. 347 (1967). Nel decidere sulla causa in questione, la Corte Suprema americana, fornì una nuova quanto evolutiva interpretazione del Quarto Emendamento della Costituzione; con riguardo alle comunicazioni tra individui, il collegio pervenne a un formale riconoscimento del diritto alla riservatezza, *dovunque* essi si trovassero.

[22] Sul punto, si veda il lavoro che ha reso celebri i giuristi di Boston, *The right to privacy*, in *Harvard Law Review*, vol. IV, n. 5, 1890, 193-220.

consumatore ha caratteristiche diverse dagli altri, al punto da rappresentare un segmento rilevante per l'analisi (*segment of one*). Dal lato dell'offerta, l'informazione personale ha dunque assunto il ruolo di fattore della produzione che contribuisce alla realizzazione di beni attagliati a bisogni individuali; per dirla con le parole dell'economista H. R. Varian, i dati personali forniscono il materiale grezzo per le analisi del comportamento dei consumatori[23]. Espressione emblematica di un'economia fondata sull'impiego di dati di natura personale è il *direct marketing*, attività con cui le imprese propongono i propri prodotti e servizi rivolgendosi ai singoli consumatori. Al riguardo, può essere utile precisare che, in taluni casi, la disponibilità dei dati personali è limitata alle sole coordinate telefoniche o elettroniche (*e-mail*) e che il trattamento consiste semplicemente nel loro uso per il contatto con i potenziali acquirenti attraverso servizi di comunicazione elettronica diretta (*unicast*); mentre, in altri, le imprese sfruttano ulteriori informazioni, acquisite nell'ambito di una preesistente e consolidata relazione con i consumatori o ricavate da fonti esterne, grazie alle quali possono ricostruire, in modo più o meno approfondito, le loro abitudini sul mercato. Merita, altresì, sottolineare come le imprese abbiano intuito l'opportunità di estendere il rapporto con i consumatori anche alla fase *post*-vendita o – se si vuole – del consumo; sul punto, va sottolineato che l'esperienza del consumo fornisce utili informazioni sulle aspettative di soddisfazione del consumatore che possono essere dedotte dallo scostamento tra queste e l'utilità del bene venduto (ossia la sua capacità di appagamento del bisogno)[24]. Di qui, facile concludere che intenzione delle imprese è quella di inquadrare il rapporto in una prospettiva di lungo periodo, in cui assicurarsi la fedeltà dei consumatori[25]. Il profilo virtuoso di questa pratica risiede nel fatto che, alla luce della condizione di

[23] Cfr. H. R. VARIAN, *L'economia politica dei motori di ricerca di Internet*, in *Rivista di Politica Economica*, vol. XI-XII, 2006, 9-25.

[24] In tal senso, R. GRANDINETTI, M. PAIOLA, *Impegno e voce dei consumatori nei processi di acquisto*, Atti del Congresso internazionale "Le tendenze del Marketing", Università Cà Foscari, Venezia, 28-29 novembre 2003.

[25] Cfr. G. RASI, *Cosa cambia per le attività produttive*, in G. RASI (a cura di) *Da costo a risorsa. La tutela dei dati personali nelle attività produttive*, Roma, 2004, 7-16.

concorrenza, il trattamento che le imprese svolgono sui dati personali ha lo scopo di interpretare i bisogni e desideri dei consumatori e di appagarli il più coerentemente possibile con la loro specifica funzione di utilità. Peraltro, rileva sottolineare come la prospettiva dell'impresa di disporre di elementi di natura personale sia collegata al ruolo di "agente relazionale" che questa deve opportunamente svolgere nell'ambiente circostante[26], di cui anche i consumatori fanno parte; qui, entra in gioco la capacità dell'impresa di produrre l'effetto voluto, vale a dire il trattamento consensuale dei dati personali. Dalla letteratura in materia emerge come il rapporto con il consumatore non possa più essere mantenuto entro lo schema verticale e transazionale tipico del modello della produzione di massa; un confronto dominato dall'impresa, in cui il consumatore – per usare un termine, forse eufemistico, di Micelli – delega a questa la funzione di produzione[27], potendo solo accogliere o respingere l'offerta senza poter intervenire nel processo di allestimento, lascia intatta quella distanza tra produzione e consumo che non garantisce l'accesso ai dati personali. Occorre allora che la relazione impresa-consumatore sia riconsiderata in chiave di convergenza tra produttore e consumatore (*prosumer*)[28]; passaggio, questo, che sul piano pratico implica un rapporto di cooperazione nella progettazione dell'offerta. In questa prospettiva, se impostata in un'ottica non opportunistica, la *partnership* con il consumatore favorisce l'accesso a informazioni rivelatrici del suo comportamento sul mercato; informazioni che, pertanto, possono aiutare l'impresa a predisporre un'offerta vicina alla soddisfazione attesa del cliente. L'approccio relazionale è ormai assurto a paradigma

[26] Cfr. E. RULLANI, *Pasquale Saraceno istituzionalista industriale*, in AAVV, *Il governo delle imprese. Pasquale Saraceno e la produzione industriale*, Padova, Cedam, 1992.

[27] Cfr. S. MICELLI, *Imprese, reti e comunità virtuali*, Milano, Etas, 2000.

[28] Cfr. P. DEGLI ESPOSTI, *La contraddizione della personalizzazione di massa all'interno delle logiche di prosumerismo*, IX Convegno nazionale AIS, Milano, 2010; G. FABRIS, *Customer Knowledge Marketing*, in *Consumatori, Diritti e Mercato*, n. 1, 2008, 91-98; G. BUSACCA, R. GRANDINETTI, G. TROILIO, *Transizione del marketing e concezione sistemico-evolutiva del consumatore*, in E. RULLANI, S. VICARI (a cura di), *Sistemi ed evoluzione nel management*, Milano, Etas, 1999.

per le imprese sottoposte a pressione concorrenziale[29], anche se non tutte lo interpretano nella prospettiva *prosumer*; con tutta probabilità, quelle più lungimiranti ne ricaveranno un vantaggio competitivo, almeno per un certo periodo.

3. Sulla natura personale della funzione di utilità del consumatore.

La caduta del paradigma fordista e la conseguente crisi della produzione di massa – siamo negli anni Settanta del secolo passato – hanno quanto meno riequilibrato il rapporto tra produzione e consumo; in altre parole, il fenomeno della frammentazione della domanda ha rappresentato un segnale dello spostamento di una parte del potere di mercato sul lato dei consumatori[30]. Da allora l'iniziale approccio verticale, orientato a condizionare la mappa delle preferenze dei consumatori per farli convergere verso pochi gruppi di prodotti omogenei, è stato superato da una domanda più autonoma, caratterizzata da un comportamento divergente, che ha imposto alle imprese un cambio di rotta: puntare alla conoscenza delle specifiche necessità del consumatore che si innescano dalla sua interazione con l'ambiente circostante. Acque decisamente meno tranquille quelle che le imprese hanno dovuto – e, in prospettiva, dovranno – affrontare, se si considera che queste necessità non sono quelle determinate dalla produzione capitalistica[31]; come a dire, che il comportamento del consumatore è mosso da *motivazioni* non più facilmente inquadrabili e standardizzabili che lo hanno reso meno regolare e prevedibile. Il passaggio dalla convergenza alla divergenza segna la fine di un'economia caratterizzata da un eccesso della domanda rispetto all'offerta (economia di scarsità) e l'inizio di una fase *post*-fordista in cui si assiste all'ingresso di nuove imprese sui mercati e al capovolgimento del rapporto dimensionale tra domanda e offerta

[29] Cfr. C. GRÖNROOS, *Quo vadis marketing? Toward a relationship marketing paradigm*, in *Journal of Marketing Management*, vol. 10, n. 5, 1994, 347-360.
[30] Cfr. W. G. SCOTT, *Il marketing nell'impresa in rete*, in B. LAMBORGHINI, S. DONADEL (a cura di), *Innovazione e creatività nell'era digitale*, Milano, 2006, 65-86.
[31] Cfr. V. PACKARD, *I persuasori occulti*, Torino, Einaudi, 1989.

(economia in eccesso di offerta). Sul lato dell'offerta si è dunque verificato un cambiamento delle politiche produttive e di vendita, decisamente orientate al consumatore e ai suoi reali bisogni[32], alle sue motivazioni quali che esse siano; il che significa che le imprese hanno dovuto seguire la disgregazione della domanda – il distacco di frammenti dal mercato di massa[33] – intuendo l'opportunità di una partizione dei consumatori in gruppi omogenei rispetto a un insieme di caratteristiche comportamentali ritenute sufficientemente stabili[34]. Peraltro, la segmentazione è apparsa ben presto insufficiente rispetto alla profondità della frammentazione, che non solo ha raggiunto il singolo consumatore, ma sembra essersi spinta oltre, esprimendo una instabilità delle sue preferenze nel tempo e nello spazio, a dispetto di ipotesi di un univoco modo di essere[35]. Di qui, la conclusione che la funzione di utilità del consumatore si discosta dal modello immaginato per un "uomo economico" per assumere valenza personale, essendo l'immagine di un comportamento di scelta che è specifico e non comune a un gruppo né tantomeno generalizzato. La disgregazione della domanda si caratterizza dunque sotto il profilo dell'utilità soggettiva[36]; vale a dire che, a parità di bisogni, i consumatori hanno funzioni di utilità diverse e dunque diversa è la

[32] Cfr. E. VALDANI, *Definizione e segmentazione del mercato per i beni industriali e di largo consumo*, Milano, Giuffrè, 1984.
[33] Cfr. G. GERKEN, *Addio al marketing*, Torino, Isedi, 1994.
[34] Cfr. M. CORNIANI, *La gestione competitiva delle bolle di domanda*, in *Simphonya. Emerging Issues in Management*, n. 1, 2002.
[35] In tal senso, v. A. BURRESI, S. GUERCINI, *Rappresentazione strategica del mercato e segmentazione in rapporto alle nuove tendenze dell'ambiente di marketing*, Atti del Convegno "Le tendenze del marketing in Europa", Università Ca-Foscari, Venezia, 2000.
[36] Il concetto di utilità soggettiva va attribuito a D. Kahneman e A. Tversky. Nell'ambito della loro *Prospect theory*, i due psicologi israeliani hanno introdotto la "funzione del valore soggettivo"; si tratta della valutazione personale che gli agenti assegnano a un insieme di possibili alternative. Al riguardo, cfr. D. KAHNEMAN, A. TVERSKY, *Prospect theory: an analysis of decision under risk*, in *Econometrica*, vol. 47, 1979, 263-291; Cfr. D. KAHNEMAN, *Maps of bounded rationality: a perspective on intuitive judgment and choice*, prolusione in occasione del conferimento del premio Nobel, 2002 (tr. it. *Mappe di razionalità limitata. Indagini sui giudizi e le scelte intuitivi*, in M. MOTTERLINI, M. PIATTELLI-PALMARINI (a cura di), *Critica della ragione Economica*, Milano, Il Saggiatore, 2005).

struttura delle preferenze sui panieri di beni giudicati idonei a soddisfare quei bisogni. Merita al riguardo precisare come tale divergenza possa caratterizzarsi sia sotto il profilo dimensionale (differenze nelle quantità) sia sul piano della varietà (ricerca di attributi diversi per beni funzionalmente uguali) sia, al limite, dal punto di vista merceologico (propensione verso beni diversi per appagare lo stesso bisogno). E ancora, la funzione di utilità va riguardata come una variabile che può assumere forme diverse in relazione alle 'sfumature' che bisogni e desideri di uno stesso consumatore possono avere in altri momenti, luoghi e condizioni. Sotto questo aspetto, la regola che descrive l'*happiness* che il consumatore trae dai beni acquistati va ricondotta all'azione delle variabili psicologiche sul comportamento; qui entra in gioco la psicologia economica che cerca di far luce proprio sugli aspetti soggettivi del comportamento, talvolta in chiave complementare ai contributi della teoria economica, ma sovente mettendone in discussione i paradigmi. Da questa prospettiva, vale osservare come il comportamento del consumatore di ricerca e selezione di merci e servizi sia il risultato della sua interazione con l'ambiente circostante o – diversamente detto – della mediazione che le variabili soggettive svolgono su quelle ambientali, sia economiche che di altra specie[37]. É, altresì, interessante sottolineare che anche la risposta del consumatore è una variabile personale – non priva di caratteri psicologici – che, a sua volta, interagisce con l'ambiente esterno influenzandone gli stimoli. In particolare, la variabile personale/comportamentale svolge una funzione correttiva o, quanto meno, orientativa dell'impresa nella prospettiva che questa possa aggiornare la propria offerta per ottenere una risposta di acquisto del consumatore che abbia un'elevata probabilità di ripetersi[38].

[37] Cfr. F. MASSARA, *In-store marketing e valore per il cliente: un modello interazionista per indagare l'esperienza d'acquisto*, Università IULM, working paper n. 7, novembre 2003, e la letteratura ivi indicata.

[38] Questa dinamica è riconducibile al modello comportamentista introdotto dallo psicologo statunitense Skinner, che esalta l'aspetto attivo del comportamento. Cfr. B. F. SKINNER, *Science and human behaviour*, New York, 1953 (tr. it. *Scienza e comportamento*, Milano, Franco Angeli, 1971).

4. Stima della funzione di utilità del consumatore e implicazioni sulla riservatezza.

La funzione di utilità del consumatore considerata nei suoi diversi aspetti – quantitativo, qualitativo, merceologico, spazio-temporale – descrive una parte della sua dimensione personale, segnatamente quella riconducibile alle scelte effettuate sul mercato. Nell'economia di varietà la disponibilità di dati sui consumatori che supportano le imprese nella ricostruzione delle funzioni di utilità personali[39] rappresenta una condizione necessaria per la loro sopravvivenza, ossia per il conseguimento di un rendimento destinato a remunerare i fattori della produzione e a ricompensare (a premiare) il rischio. A tal riguardo, merita osservare come le Ict costituiscano, tra l'altro, un potente strumento di rilevazione di dati personali per la costruzione del profilo di un consumatore esplicativo delle sue preferenze e quindi di ciò che egli considera più utile; la carta commerciale è lo strumento forse più diffuso nel mercato *retail* – in particolare nella grande distribuzione – che utilizza queste tecnologie per raccogliere dati sulle abitudini del suo utilizzatore. Il patrimonio informativo che questo strumento dischiude, consente alle imprese di conoscere aspetti del comportamento nel tempo – la composizione dei panieri di spesa individuali, la loro dimensione, la frequenza di acquisto – e di individuare gli stimoli più appropriati per non diminuire le utilità dei consumatori così da mantenere con questi il rapporto di scambio; ad esempio, l'analisi dei dati personali può fornire a un *retailer*, presente sul territorio con più punti vendita, utili elementi per valutare la convenienza di una differenziazione geografica dell'offerta sotto il profilo della marca, delle quantità o delle politiche promozionali. In una prospettiva di *retention* questa pratica è spesso sostenuta da

[39] La teoria economica assume che l'utilità provata dal consumatore va posta in relazione alla disponibilità simultanea di un insieme di beni diversi, idonei a soddisfare una combinazione di bisogni (v. sul punto A. GRAZIANI, *Teoria economica. Prezzi e distribuzione*, Napoli, Edizioni scientifiche italiane, 1985, 163). Sotto questo aspetto, è ragionevole presumere che un'impresa sia impegnata a stimare un ramo della funzione di utilità del consumatore, alla luce della considerazione che essa, verosimilmente, non fornisce tutti i beni che concorrono alla sua soddisfazione.

programmi di ricompensa (sconti, informazioni sui beni, premi, servizi)[40], i quali – vale la le pena sottolinearlo – sono diventati fattori di connotazione dell'offerta al punto da essere al centro delle strategie competitive dei distributori rivali, e che gli stessi pongono in essere in forma di differenziazione o di imitazione[41]. Nel quadro di questi programmi, la riduzione dei prezzi conserva sempre il suo *appeal* sugli acquirenti; al riguardo, va sottolineato come manovre del genere siano suscettibili di determinare un incremento di soddisfazione sul lato della domanda[42]. Sotto altro profilo, è interessante rilevare come gli incentivi associati alle carte elettroniche commerciali possano essere riguardati come forme di remunerazione del costo opportunità dei consumatori determinato dalla *loss of privacy*, ossia dalla rinuncia alla riservatezza dei dati che li riguardano. Con lo spostamento in Internet delle relazioni tra imprese, famiglie, istituzioni, organizzazioni, la raccolta di informazioni personali si realizza attraverso i mezzi, le tecnologie e i *device* impiegati in tale ambito; in particolare, nel rapporto di *e-commerce* tra impresa e consumatore la Rete sostituisce il sistema digitale della *fidelity card* nell'acquisizione delle informazioni commerciali personali. Peraltro, sappiamo dall'esperienza e dalla letteratura che in questa e altre circostanze Internet è sede di *profiling* dei suoi utilizzatori, attività essenziale per la raccolta pubblicitaria *on line*. Al riguardo, va rilevato che, alla stregua dei *media* tradizionali, il mercato generato da Internet mostra una struttura a due versanti (*two sided market*). Su un lato si assiste alla fornitura di servizi e contenuti agli utenti da parte dei *provider*; sull'altro si realizza la raccolta della domanda di spazi pubblicitari

[40] Cfr. B. LUCERI, *Il comportamento del consumatore di fronte al micromarketing*, Atti del Congresso internazionale "Le tendenze del marketing", Università Cà Foscari, Venezia, 2003.

[41] Cfr. G. LUGLI, C. ZILIANI, *Dalle carte fedeltà a Internet: l'evoluzione del micro marketing*, in *Micro & Macro Marketing*, n. 1, 2001, 115-142.

[42] Sul punto, vale la pena precisare che il prezzo è una variabile esplicativa del comportamento e non dell'utilità percepita dal consumatore che, invece, è il prodotto della sua interazione con le caratteristiche del bene che avviene nella fase del consumo. D'altro canto, la teoria economica del consumo ha postulato un legame indiretto tra prezzi e soddisfazione. La riduzione dei prezzi dei beni determina un aumento della capacità di spesa del consumatore; questo esito consente l'acquisto di maggiori quantità di beni che determinano un incremento di soddisfazione.

che, tenuto conto anche dei prezzi, dipende dal flusso e dalle caratteristiche dei visitatori del versante dei servizi e dei contenuti. Ma, a differenza dei *media* storici, con riferimento ai quali, elaborando dati campionari di *audience*, è possibile solo costruire macro-segmenti di consumatori a cui attribuire preferenze omogenee, Internet consente la rilevazione di una massa di dati più ampia riguardante abitudini e preferenze di singoli visitatori; di qui, è facile concludere sulla maggiore efficacia dei messaggi pubblicitari in Rete rispetto a quelli veicolati attraverso le piattaforme tradizionali[43]. I fornitori di servizi di ricerca in Internet (*search engines*) sono esempi tipici di imprese i cui ricavi derivano prevalentemente dal versante della raccolta pubblicitaria con l'offerta agli inserzionisti di spazi (*slot*) nei quali è collocato un collegamento che rinvia a messaggi pubblicitari in qualche misura correlati ai contenuti della ricerca dell'utente-consumatore[44]. L'acquisto dello spazio contenente il *link* al proprio sito riposa sulla presunzione che l'utente che effettua una determinata ricerca possa essere interessato all'attività svolta dall'impresa inserzionista[45].

Da una prospettiva di mercato, non si può non riconoscere che la raccolta e l'elaborazione di dati personali, volte alla definizione di profili individuali, possa avere ricadute positive anche per i consumatori, segnatamente sotto il profilo dell'utilità dei beni proposti. L'aspetto critico di simili trattamenti sta nel fatto che questi si espongono al rischio di una diversa percezione allorché vengono effettuati in condizioni di scarsa trasparenza e perfino senza che gli interessati ne siano al corrente, privandoli della possibilità di opposizione[46]. Qui, il diritto è chiamato a svolgere la sua funzione di

[43] cfr. G. MACCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in *Dir. Inf. Inf.*, n. 3, 2001, 425-444.

[44] Cfr. C. SHAPIRO, H. R. VARIAN, *Information rules. Le regole dell'economia dell'informazione*, Milano, Etas, 1999.

[45] Cfr. N. MECCHERI, *Schemi di prezzo su Internet: accesso alla rete e pubblicità sui motori di ricerca*, in *L'industria*, n. 4, 2009.

[46] La rilevazione di dati personali sui consumatori con le *fidelity card* si compie con una registrazione elettronica che associa alla carta del cliente – e dunque ai dati personali identificativi – la spesa da questo effettuata. L'acquisizione in Rete di elementi personali si realizza con l'impiego di *software* (*cookie*, *data log*, …) che depositano nelle apparecchiature informatiche degli utilizzatori algoritmi che

tutela dei dati personali, affinché il loro trattamento – se pure necessario per l'attività delle imprese e per la crescita economica – possa svolgersi in un quadro di regole che assicuri la trasparenza e l'esercizio dell'autodeterminazione informativa. Con riguardo alla pratica del *profiling* svolto attraverso mezzi di comunicazione elettronica, la disciplina che ne regola l'adozione è riconducibile al quadro normativo europeo, segnatamente quello stabilito dalla direttiva 2002/58 concernente il trattamento dei dati personali nel settore delle comunicazioni elettroniche. Merita al riguardo osservare che detta disciplina non vieta l'uso *per sé* di algoritmi informatici idonei a rilevare informazioni personali; questi sono ammessi per scopi legittimi, come l'efficacia di una comunicazione pubblicitaria oppure la facilitazione della fornitura di servizi internet e servizi della società dell'informazione o, ancora, l'identificazione degli utenti che effettuano transazioni *on line*, sempre che gli interessati ne siano a conoscenza e possano autorizzare o, comunque, rifiutare l'installazione di dispositivi nelle loro apparecchiature informatiche (v. considerando n. (24) e n. (25)). Sul fronte interno, in particolare della prassi del Garante, meritano menzione i provvedimenti con cui l'autorità di controllo ha stabilito le regole per il trattamento dei dati personali svolto sia da operatori commerciali che si avvalgono dell'uso di carte fedeltà digitali[47] sia da fornitori di servizi di comunicazione elettronica[48] sia, ancora, da *provider* che forniscono servizi e contenuti attraverso Internet[49].

---

memorizzano percorsi, interrogazioni, preferenze, transazioni, e che possono risalire anche all'indirizzo della posta elettronica. Cfr. V. CARIDI, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali*, in *Dir. Inf. Inf.*, n. 4-5, 2001, 763-783; P. GUARDA, *Sicurezza dei pagamenti e privacy nell'e-commerce*, in *Diritto dell'Internet*, n. 1, 2005, 91-101.

[47] Cfr. Garante per la protezione dei dati personali, Provvedimento del 24 febbraio 2005, *fidelity card e garanzie per i consumatori*, in *Boll.* n. 58/2005.

[48] Cfr. Garante per la protezione dei dati personali, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione*, in *G. U.* n. 159 del 11 luglio 2009.

[49] Cfr. Garante per la protezione dei dati personali, Provvedimento del 22 luglio 2010, *Concorsi online e web radio*, in *Boll.* n. 118/2010; Provvedimento del 15 luglio 2010, *Raccolta di dati via Internet per finalità promozionali*, in *Boll.* n.

Il quadro testé tratteggiato introduce un *trade off* 'classico' della società dell'informazione; una situazione, cioè, che pone a confronto interessi e diritti legittimi ma tra loro in conflitto, segnatamente la libera circolazione e la riservatezza dei dati personali. Si rende pertanto necessario un bilanciamento che, in questo caso, è riconducibile alla scelta della regola che stabilisce i termini in cui le organizzazioni possono avere accesso ai dati personali. Seguendo Lessig, il *trade off* posto dai dati personali può essere ricondotto al confronto tra il principio di libertà e il diritto al controllo o, se si vuole, tra l'accesso libero e quello, in qualche misura, vincolato[50].

5. Sulla circolazione dei dati personali nella società dell'informazione.

L'informazione costituisce una risorsa essenziale per gli scopi perseguiti dalla politica europea. Tra questi spicca, per le sue implicazioni di crescita economica e di competitività, la realizzazione e il funzionamento del mercato interno[51]. L'accesso all'informazione è funzionale allo sviluppo della *conoscenza* dell'individuo[52], ossia della sua capacità di comprensione dell'ambiente, risultante dall'accumulo e dall'elaborazione di informazioni, che può impiegare nella funzione del lavoro e, più in generale, nelle attività che

118/2010; Provvedimento del 10 maggio 2006, *Consenso al trattamento in Internet e utilizzo dei dati per finalità promozionali*, in *Boll.* n. 72/2006.

[50] Cfr. L. LESSIG, *The future of ideas*, New York, 2001.

[51] In tal senso, si veda la risalente Decisione 84/567/CEE, *che adotta un programma comunitario per lo sviluppo del mercato europeo dell'informazione specializzata in Europa*, in *GU* L 314 del 4 dicembre 1984, secondo e terzo considerando: "[…] a livello mondiale, l'informazione è diventata uno dei fattori primari dell'attività economica e […] un uso efficace dell'informazione è uno degli elementi essenziali della crescita e della competitività economiche;". "[…] il processo di integrazione europea dipende sempre di più dall'esistenza, tra l'altro, di un flusso di informazioni efficace all'interno di tutti gli Stati membri e tra questi e dall'accesso a questa informazione;".

[52] Cfr. D. FORAY, *L'economia della conoscenza*, Bologna, 2006, 81 ss; v. anche V. ZENO-ZENCOVICH, F. MEZZANOTTE, *Le reti della conoscenza: dall'economia al diritto*, in *Dir. Inf. Inf.*, n. 2, 2008, 141-171.

caratterizzano la sua partecipazione alla società; mentre la diffusione dell'informazione facilita i flussi delle merci, dei servizi, delle persone e dei capitali e, con essi, la coesione economica, sociale e territoriale. L'avvento di Internet e, più in generale, l'introduzione delle Ict ha determinato il trasferimento più veloce ed efficiente di elevati volumi di dati, a dispetto dei vincoli spaziali e temporali, incoraggiando un'economia in Rete anche attraverso la generazione di nuovi servizi e nuove prestazioni; condizione, questa, preconizzata, sia pure con ottiche diverse, da autori del calibro di Jeremy Rifkin, Manuel Castells, Nicholas Negroponte. Al riguardo, va osservato che lo spostamento nel cyberspazio delle attività economiche favorisce, tra l'altro, quell'evoluzione dell'economia, già in atto *off line*, in cui gli scambi riguardano, in quantità crescenti, beni connessi all'impiego del tempo libero[53]. Sul fronte dei nuovi servizi, le esperienze di Google, Microsoft, You Tube, Facebook, testimoniano contributi alla crescita economica resi con la fornitura di servizi e prodotti strettamente connessi all'uso della Rete – si pensi ai servizi internet e ai *software* di accesso a Internet – altrimenti non realizzabili. La circolazione delle informazioni ha effetti anche sotto il profilo della concorrenza; in tale condizione, si riduce l'asimmetria informativa tra le imprese e, come conseguenza, aumenta il grado di concorrenza. Al contrario, una scarsa movimentazione delle informazioni non fa che favorire situazioni di dominanza o di concentrazione del mercato, in cui l'impresa dominante o le poche imprese che controllano il mercato solitamente dispongono di un vasto patrimonio informativo sui consumatori; in questi casi, non vanno sottovalutati i rischi di abuso di sfruttamento o di coordinamento anticompetitivo. Sulla circolazione delle informazioni, non va sottaciuto come già la teoria economica neoclassica, sia pure esaltando un modello di concorrenza *perfetta*, ne avesse messo in luce il ruolo cruciale per il funzionamento del meccanismo concorrenziale; e come la concorrenza reale – quella fondata sulla differenziazione del prodotto – non smentisca tale presupposto, caratterizzandosi per la propensione delle imprese alla

[53] Si veda, al riguardo, J. RIFKIN, *L'era dell'accesso*, Milano, Mondadori, 2000; G. SCORZA, *Internet, il mercato, i consumatori e le regole*, in *Consumatori, Diritti e Mercato*, n. 1, 2010, 7-18.

scoperta di aspetti specifici del consumatore per adattarvi le proprie offerte; questa dinamica determina benefici per i consumatori sia sotto il profilo della qualità dei beni posti sul mercato sia perché, in condizioni di maggiore scelta, questi possono esigere dalle imprese informazioni sulla gamma e sulle caratteristiche dell'offerta. In altre parole, la circolazione delle informazioni di interesse per le imprese innesca il meccanismo della concorrenza che, a sua volta, riduce le asimmetrie informative anche tra domanda e offerta e aumenta la trasparenza del mercato[54].

È dunque pacifico concludere come la movimentazione delle informazioni (personali e non) sia una caratteristica fondamentale della società dell'informazione e della sua economia, i cui effetti non sono di poco conto. In questa prospettiva, il diritto comunitario assicura la circolazione delle informazioni compresi i dati personali; se pure, per questa categoria, la libertà di trasferimento – e, più in generale, la libertà del loro trattamento – va inquadrata in una condizione di equilibrio con i diritti fondamentali della persona[55], nei quali rientra il diritto alla riservatezza. Il bilanciamento tra i contrapposti interessi è certamente un'operazione critica: se una disciplina del trattamento dei *personal data* appare necessaria per evitare comportamenti che possono andare oltre i limiti tollerati dai consumatori – e che, come tali, possono risultare abusivi – non va neppure sottaciuto il fatto che l'attività economica non può realisticamente prescindere dalla disponibilità dei dati personali né può essere trascurato il beneficio sociale, ossia – per dirla in termini tecnici – le esternalità positive che la loro circolazione può

[54] Cfr. G. TESAURO, *Competizione economica: i vantaggi della protezione dei dati*, in G. RASI (a cura di), *Da costo a risorsa*, *op. cit*., 213-219.

[55] Al riguardo, cfr. Direttiva 95/46/CE, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, in *GUCE*, L 281, del 23 novembre 1995, al terzo considerando: "[…] l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona;". Cfr. anche il trattato sul funzionamento dell'Unione Europea, art. 16.

determinare[56]. Le norme in materia non dovrebbero pertanto costituire ostacoli o *bottleneck* al passaggio verso l'economia dell'informazione; altrimenti il rischio è quello di un ritorno ai metodi di 'somministrazione' delle offerte, caratteristici del mercato di massa. Sul punto, rileva osservare come, alla luce del quadro normativo comunitario – il riferimento è alla direttiva 95/46, che non lascia dubbi sul modo di intendere l'approvazione al trattamento dei dati personali e sugli orientamenti in tema di circolazione dei dati personali – le ragioni di chi è a favore del mercato si sono appuntate sull'alternativa di un regime che possa eliminare alcune rigidità nel rapporto tra impresa e consumatori; regime in virtù del quale le imprese potrebbero svolgere liberamente il trattamento dei dati personali per scopi commerciali, purché i consumatori interessati siano preventivamente informati e fintantoché questi non decidano di manifestare il diritto all'autodeterminazione su tali dati, ponendo restrizioni al trattamento. Una simile soluzione giuridica riposa dunque su un principio di disponibilità *ex ante* dei dati personali che, rispetto alla citata direttiva del 1995, modifica il senso che può essere dato all'assenza di un pronunciamento dal lato dei consumatori; detto principio ammette, cioè, l'assunzione di un'implicita approvazione, per le imprese, a procedere al trattamento, mentre dal lato degli interessati comporta un'esplicita azione per chi intende opporsi allo stesso (o ad una sua parte). Le aperture in tal senso offerte dalla legislazione europea[57] hanno prestato il fianco, nel nostro Paese, a un

[56] In tal senso, A. PALMIERI, *Personal data privacy nell'information age tra diritti, regole e mercato: spunti di riflessione*, in *Politeia*, n. 59, 2000, 102-121.

[57] Cfr. Direttiva 97/66/CE, *sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni*, in *GUCE* L 24 del 30 gennaio 1998, art. 12, paragrafo 2; Direttiva 2000/31/CE, *relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)*, in *GUCE*, L 178 del 17 luglio 2000, art. 7; Direttiva 2002/58/CE, cit., considerando n. (42) e art. 13, paragrafo 3. Vale precisare che la direttiva *e-commerce* contemplava la possibilità, per gli Stati membri, di adottare il criterio *opt-out* con la previsione di un registro di opposizioni per l'invio di comunicazioni commerciali, non richieste in anticipo, anche attraverso il servizio di *mail* elettronica; mentre la direttiva del 2002 ha eliminato il servizio di corrispondenza elettronica dall'applicazione del predetto criterio, introducendo tuttavia una deroga nel caso in cui l'impresa intenderebbe commercializzare prodotti

dibattito sul *trade off* tra mercato e privacy non poco controverso in ragione di una tradizione politica e giuridica prevalentemente spostata sui diritti dei consumatori; dibattito che, malgrado ciò, si è concluso con l'adeguamento del Codice della privacy all'equilibrio testé tratteggiato, avvenuto con il decreto-legge n. 135 del settembre 2009 e con la legge di conversione n. 166 del novembre 2009[58]. Con questi passaggi, nei limiti contemplati dalla direttiva n. 58 del 2002, l'ordinamento nazionale ha adottato l'opzione negativa, c.d. *opt-out*, con riguardo all'attività di "marketing telefonico", rivestita di un opportuno registro (*Robinson list*) per consentire agli utenti di esprimere, iscrivendosi, il divieto di trattamento dei propri dati telefonici per lo svolgimento dell'attività di contatto.

I margini concessi dal diritto comunitario agli Stati membri per l'applicazione della regola in discorso lasciano trapelare l'interesse del legislatore al «trattamento» consistente nella circolazione dei dati personali, in ragione del fatto che detta circolazione agevola gli scambi economici transfrontalieri; interesse che, invero, si coglie fin dai documenti giuridici degli anni '80 e '90 del secolo passato, adottati in tal senso[59]. Al riguardo, non va sottaciuto che la previsione di un consenso *ex ante* – che si può considerare alla stregua di un permesso di accesso a una proprietà privata[60] – finisce per incidere

---

o servizi analoghi a quelli per i quali ha già ottenuto, dai propri clienti, le coordinate elettroniche.

[58] Cfr. Legge 20 novembre 2009, n. 166, *Conversione in legge, con modificazioni, del d. l. 25 settembre 2009, n. 135, recante disposizioni urgenti per l'attuazione di obblighi comunitari e per l'esecuzione di sentenze della Corte di giustizia delle Comunità europee*, in *G.U.* n. 274 del 24 novembre 2009, Suppl. Ord. n. 215/L. In particolare si veda l'art. 20-*bis* (Adeguamento alla normativa comunitaria in materia di tutela della vita privata nel settore delle comunicazioni elettroniche, di cui alla direttiva 2002/58/CE) del Testo del decreto-legge 25 settembre 2009, n. 135 coordinato con la legge di conversione 20 novembre 2009, n. 166.

[59] Tra tutti, si veda la Convenzione n. 108/1981, adottata a Strasburgo il 28 gennaio 1981.

[60] Cfr. G. CLERICO, *Proprietà intellettuale, esternalità e rendita*, in *Economia, Società e Istituzioni*, n. 1, 2006.

L'inquadramento dei dati personali nel diritto di proprietà descrive un modello di tutela di matrice liberale-borghese che contempla la classificazione delle informazioni personali alla stregua di beni economici. A tale schema si contrappone il modello europeo che riconduce la protezione dei dati personali a un diritto della

all'origine dei potenziali flussi, in tal caso assumendo inevitabilmente la connotazione di una barriera alla formazione del mercato interno; e che, nella verosimile prospettiva che la circolazione si svolga in Rete la predetta opzione positiva, oltre a non essere risolutiva dei problemi di trasparenza che in tale contesto si pongono, introduce importanti interrogativi sulle implicazioni verso il commercio e la pubblicità elettronici. Sappiamo, al riguardo, come l'impiego di taluni *software* (c.d. *cookie*) sia necessario per identificare i consumatori che effettuano transazioni *on line*. Un siffatto trattamento andrebbe in qualche misura assecondato, sotto il profilo giuridico, anche in ragione dell'opportunità che offre per calibrare, sull'utilità del consumatore, pubblicità e offerte *on line*[61]. In questa prospettiva, la protezione dei dati personali deve piuttosto caratterizzarsi come potere di controllo dell'interessato sui possibili trattamenti, compresa la circolazione. Qui, il diritto è chiamato a fare la sua parte, vale a dire ad assicurare le condizioni affinché ciascun individuo possa esplicare la funzione del controllo. Di fronte a questa condizione giuridica la scelta dell'opzione cui sottoporre il trattamento finisce con l'apparire indifferente sul piano della tutela; circostanza, questa, che, una volta di più, suggerisce l'adozione dell'opzione che pone meno limiti alla circolazione dei dati personali. Altro aspetto che merita di essere evidenziato riguarda le implicazioni di efficienza dell'introduzione di un registro delle opposizioni al trattamento; l'obbligo, per le imprese, della sua consultazione, invero si trasforma in uno strumento di risparmio dei costi di comunicazione e di riduzione dell'incertezza

personalità che esclude la separazione tra il soggetto titolare del diritto e l'oggetto del diritto medesimo (la personalità, se pure parte di questa è rappresentata nella forma di dati digitali). La questione dell'inquadramento giuridico dei dati personali probabilmente è destinata a restare insoluta.

[61] Sulla necessità della circolazione dei dati personali per lo sviluppo del commercio elettronico cfr. M. BELLABARBA, *Il livello di protezione della privacy negli U.S.A. é davvero adeguato?*, in www.privacy.it/bellabarba01.html (visitato il 26 agosto 2010); R. IONTA, *Le comunicazioni elettroniche e il diritto alla riservatezza. Direttive comunitarie e ordinamento nazionale*, in *AmbienteDiritto.it*, 2004, (articolo reperito all'indirizzo www.ambientediritto.it/ dottrina/Dottrina%202004/ comunicazioni_ elettroniche.htm, visitato il 26 agosto 2010).

sulla domanda[62]. Va peraltro osservato come un simile esito economico non sia esclusivo dell'opzione negativa, ma possa realizzarsi anche in condizioni di consenso preventivo. L'aspetto critico di un tale regime risiede, però, nel fatto che non si può escludere che l'elenco di nominativi di persone non interessate a ricevere informazioni e proposte commerciali, possa rivelarsi sovrastimato; in altre parole, una quota dei contatti che non possono essere effettuati, per assenza di consenso, potrebbero non essere realmente indesiderati, il che, assieme a un risparmio di costi, determinerebbe anche minori ricavi.

6. Conclusioni.

Che l'economia abbia bisogno dei dati personali è un fatto ormai pacifico, se pure l'impressione è che – economisti a parte – la comunità degli addetti ai lavori sia più sensibile alla protezione di tali dati piuttosto che alla necessità delle imprese di poterli trattare sia pure in una prospettiva virtuosa. Al di là del rapporto tra diritti fondamentali della persona e diritti economici delle imprese, un simile – e, tutto sommato, comprensibile – atteggiamento, non può non essere messo in relazione al comportamento sia di talune imprese dominanti la cui posizione di mercato è collegata al trattamento (di dubbia trasparenza) di dati individuali[63] sia di tali altre che, pur non essendo dominanti, pongono in essere trattamenti abusivi nei riguardi dei consumatori per conquistare quote di mercato[64]. A dispetto di ciò, le porte dischiuse dal diritto comunitario a favore di meccanismi meno

[62] Sul punto cfr. A. ACQUISTI, *Privacy*, in *Rivista di Politica economica*, maggio-giugno 2005, 333-334. Una interessante testimonianza in tal senso, proveniente dal mondo dell'impresa, è fornita da M. COSTA, *Investire in privacy per lo sviluppo di nuovi prodotti e servizi*, in G. RASI (a cura di), *Da costo a risorsa*, *op. cit*., 348-355.

[63] Caso noto è quello della società Google che occupa una posizione dominante nel mercato dell'intermediazione nella raccolta pubblicitaria *on-line*. Al riguardo cfr. Autorità garante della concorrenza e del mercato, Provvedimento n. 20224, caso n. A420, *FIEG/Google*, in *Boll.* n. 34/2009.

[64] Cfr. Garante per la protezione dei dati personali, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione*, cit.

comprimenti della libertà di utilizzo dei dati personali rappresenta, per i paesi membri, un segnale di incoraggiamento alla loro introduzione negli ordinamenti interni a beneficio dell'attività economica delle imprese, in particolare di quella di contatto dei consumatori attraverso servizi di comunicazione telefonica; l'applicazione di siffatti meccanismi va peraltro considerata alla luce dei principi di trasparenza e di autodeterminazione informativa volti a salvaguardare i consumatori. La disciplina appare, invece, più protettiva nel caso in cui il trattamento dei dati personali contempla l'impiego del servizio di corrispondenza elettronica (*e-mail*); una scelta, questa del legislatore, che, con tutta probabilità, va ascritta alla piaga dello *spamming*, ma a cui va anche riconosciuta la previsione di una deroga nelle circostanze indicate dalla direttiva *e-privacy*[65]. Da un punto di vista di mercato, l'auspicio non può che essere quello di un'estensione giuridica almeno della discrezionalità degli Stati membri di applicare l'opzione negativa anche ai casi in cui gli indirizzi *e-mail* siano nella disponibilità delle imprese senza un esplicito consenso[66]; in altre parole, di un ritorno agli orientamenti della direttiva *e-commerce* di fine secolo, in cui era chiaro l'intento del legislatore di incoraggiare una regolazione del trattamento che non costituisse una barriera allo sviluppo del commercio elettronico. Prospettiva non impossibile se inquadrata nell'ambito di una *lex informatica* – o di un *code* per dirla *à la* Lessig[67] – che possa essere il frutto di una opportuna integrazione

[65] Cfr. Direttiva 2002/58/CE, cit., art. 13, parag. 2. Si tratta del caso in cui le imprese dispongono delle coordinate elettroniche dei propri clienti ottenute con il loro consenso nell'ambito di un rapporto commerciale precedentemente instaurato. In questa condizione, le imprese possono utilizzare gli indirizzi già acquisiti per scopi di commercializzazione di altri, analoghi, beni, sempre che i destinatari possano opporsi in qualsiasi momento al trattamento. Rileva notare come, diversamente dai casi in cui l'adozione dell'opzione negativa è rimessa agli ordinamenti interni (v. art. 13, parag. 3), la norma in argomento è di diretto recepimento.

[66] Circostanza facilitata da Internet, come posto in evidenza dal Garante per la protezione dei dati personali. Al riguardo, v. *Spamming. Regole per un corretto invio delle e-mail pubblicitarie - Provvedimento generale*, in *Boll.* n. 39/2003; *Reti telematiche e Internet - Comunicazione politica, e-mail, atti e documenti pubblici conoscibili da chiunque*, in *Boll.* n. 16/2001.

[67] Sull'argomento, v. L. LESSIG, *Code and other laws of Cyberspace*, New York, 1999.

tra tecnologia e diritto idonea quanto meno a ridimensionare i casi di comunicazioni classificabili come *send phenomenal amounts of mail*. Al riguardo, merita rilevare come le indicazioni in tal senso, a suo tempo fornite dal legislatore comunitario agli Stati membri[68], abbiano trovato un generale seguito nei *service provider* che hanno approntato misure tecnologiche *anti-spam* e adottato codici di buona prassi per il contrasto al fenomeno[69]. Questa e altre esperienze di difesa tecnologica dei diritti (si pensi ai rimedi *software* ideati per proteggere i minori nell'uso di Internet o per impedire l'appropriazione di contenuti presenti in Rete che sono oggetto di proprietà intellettuale) lasciano dunque ben sperare sull'approccio alla regolazione tecnica; approccio che esprime un atteggiamento propositivo della legislazione, che cioè non subisce la tecnologia, limitandosi a censurare i trattamenti illeciti che essa può abilitare, ma svolge una funzione di guida del progresso tecnologico secondo una logica di compatibilità con le norme giuridiche prefissate[70]. In un contesto come la società dell'informazione, in cui la tecnologia può farsi strumento del diritto per assicurare, nei limiti di un ragionevole equilibrio, la libertà economica e gli interessi dei consumatori, invero il consenso *ex ante* ed esplicito inizia a perdere il requisito della necessità; tanto più se si considera che, nell'ipotesi di adozione di un'opzione negativa e nella condizione di inibizione tecnologica di trattamenti occulti e di fenomeni come lo *spam*, la presenza di un'autorità preposta alla protezione dei dati personali costituisce pur sempre una forma di tutela dell'interessato da eventuali comportamenti illeciti[71]. Ulteriore tutela – che va considerata in termini di disincentivazione di detti comportamenti – è offerta dallo strumento dell'azione collettiva per il risarcimento del danno

[68] In tal senso, Direttiva 2000/31/CE, cit., al considerando n. (30).
[69] Cfr. Commissione delle comunità europee, *Sulla lotta contro le comunicazioni commerciali indesiderate (spam), i programmi spia (spyware) e i software maligni*, comunicazione COM(2006) 688, del 16 novembre 2006.
[70] Cfr. S. RODOTÀ, *Tecnologie e diritti*, Bologna, Il Mulino, 1995.
[71] In tal senso, cfr. V. CUFFARO, *A proposito del ruolo del consenso*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998.

procurato ai consumatori[72], introdotto nel nostro ordinamento dalla legge finanziaria 2008. Con riguardo alle comunicazioni ripetute e non richieste – dunque, presumibilmente indesiderate – merita menzionare la disciplina delle pratiche commerciali sleali a cui tale fattispecie è sottoposta (essendo qualificata come pratica *aggressiva*[73]). L'istituto del consenso appare ancora meno giustificato se, alle precedenti riflessioni, si aggiunge che la concorrenza monopolistica e la prospettiva del (più efficiente) commercio elettronico non lasciano spazio a manovre sui dati personali che possano implicare, per le imprese, rischi di abbandono della domanda e, con esso, di perdita di quote di mercato. Sotto questo aspetto, vale la pena aggiungere che la Rete offre ai *cyber-consumer* strumenti idonei a puntellare il loro potere di mercato; le soluzioni cosiddette *web 2.0*, ad esempio, forniscono ai consumatori un supporto formidabile sotto il profilo informativo, idoneo a disincentivare comportamenti delle imprese non trasparenti nella raccolta e nell'uso dei dati personali.

Il valore che i dati personali hanno assunto nel delinearsi di queste situazioni di mercato e la funzione vincolante che il consumo ha acquisito nei confronti della produzione, sono fatti che suggeriscono alle imprese un patto con i consumatori da cui entrambe le parti possono trarre beneficio, vale a dire un ragionevole profitto per l'una e un'apprezzabile utilità (soddisfazione) per l'altra. In questa prospettiva, il mercato è destinato a rappresentare un ambiente tutt'altro che ostile per la riservatezza dei dati personali. Peraltro, è opportuno che, anche nella società dell'informazione, l'opzione positiva vada mantenuta nei casi in cui l'opposizione *ex post* appare veramente poco adeguata per la tutela della privacy. Si pensi alle situazioni commerciali in cui i dati oggetto del trattamento minimo necessario, o risultanti da questo, hanno natura sensibile; in questi

[72] Sul ricorso alla *class action*, v. le lungimiranti osservazioni di D. D'AGOSTINI, *A che punto è la lotta allo spam ?*, in *Ciberspazio e Diritto*, vol. V, n. 3, 2004.

[73] Al riguardo, cfr. Direttiva 2005/29/CE, *relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio*, in *GUUE*, L 149 del 11 giugno 2005, Allegato I.

casi, va da sé che per un trattamento aggiuntivo, ad esempio il trasferimento a soggetti diversi dall'interessato, non deve sussistere alcun dubbio sul consenso di quest'ultimo.

Il Lobbying “legistico-giuridico”: un'attività da centro studi del terzo millennio

di Antonella Romano [(*)]

SOMMARIO: 1. Dal *lobium* medievale all’atrio dell'hotel *Willard di Washington*. – 2. Perché e come le lobby possono far bene alla democrazia. – 3. Tra il dire e il fare c’è di mezzo l’Italia. – 4. Parola d’ordine? Trasparenza!

1. Dal *lobium* medievale all’atrio dell'hotel *Willard* di *Washington*.

Anello di congiunzione tra le decisioni pubbliche e gli interessi privati, il *lobbying* non ha ancora trovato il suo posto nel mondo. O meglio, ci è riuscito solo in una parte, ed in parte. Da un primo – e nemmeno troppo attento – esame dello stato attuale di avanzamento delle norme e delle prassi che disciplinano l’attività di *lobbying* nei sistemi parlamentari delle democrazie moderne, si evince che i paesi con norme e regolamenti specifici che disciplinano l'attività dei lobbisti e gruppi d'interesse sono più l'eccezione che la regola. “Procedere senza cedere alle lobby” sembra essere il *leitmotiv*, antico e consumato, di un cambiamento culturale, politico e sociale mai avvenuto. Partorito nel fecondo atrio dell'hotel *Willard* di *Washington*, dove alla fine dell'Ottocento l'allora presidente degli Stati Uniti Ulysses Grant riceveva persone e portavoce di gruppi che ponevano richieste al governo, il nome “lobby” venne presto registrato nella *black list* del pregiudizio pubblico. Non passò molto tempo prima che la stampa dell’epoca iniziasse a dipingere i lobbisti come losche figure, con tanto di barba e lingua biforcuta, che corrompevano i parlamentari, influenzando le loro scelte politiche.

Da qui alla totale identificazione tra lobby e corruzione il passo è breve. La percezione di questa attività cambiò radicalmente e

[(*)] Dottore in Scienze Politiche e delle Relazioni Internazionali. Specializzanda in *Law And Economics*, presso la LUISS Guido Carli; Istituto Italiano per la Privacy.

rapidamente nell'opinione pubblica e nella cultura della politica degli americani, legata com'era allo slogan delle "tre B"coniato dal cronista parlamentare Edward Winslow Martin. Secondo questo slogan lobbismo significherebbe *broads, booze and bribes* (cioè bambole, bottiglie e bustarelle). In realtà la parola lobby ha ben più nobili (e decorose) origini. Viene dal termine latino medievale *lobium*, che significa "chiostro", un luogo che evoca qualcosa di più alto di una sala d'albergo americana o di un corridoio del parlamento inglese. Gianfranco Pasquino, nell'autorevole Dizionario di Politica, diretto da Norberto Bobbio e Nicola Matteucci, sostiene che per *lobbying* debba intendersi un'attività, o meglio un processo, per mezzo del quale "i rappresentanti di gruppi di interesse, agendo da intermediari portano a conoscenza dei legislatori, dei *decision makers*, i desideri dei loro gruppi."[1]. Il *lobbying* è questo: la risposta moderna (ma non troppo) alla necessità di aggregazione e partecipazione di alcuni individui, che spinge l'esito del processo politico verso il centro dello spazio politico. E' un meccanismo tra meccanismi.

Altrettanto complessa appare anche la questione riguardo alla definizione di ciò che costituisca un lobbista ed alla sua esistenza, legittima o meno. In particolare, può rivelarsi centrale, nel gioco politico della regolamentazione, la cultura politica di un paese, tanto che a volte è proprio questa componente endogena a determinarne il successo o il fallimento (Giappone ed Italia *docet*).

Spesso le regole mancano, ma non le eccezioni. Se da un lato, Germania e Regno Unito piuttosto che perdersi in chiacchiere (e definizioni) hanno preferito "ritrovarsi" nelle tranquille acque della regolamentazione, d'altra parte (e dall'altra parte) anche Stati Uniti e Canada sono riusciti a superare brillantemente l'impasse, introducendo una regolamentazione legale dei lobbisti. Negli *States* la promozione di interessi privati non solo è legittima: è garantita dalla Costituzione grazie al Primo Emendamento, sulla libertà d'opinione e di stampa, che vieta di promulgare leggi "*abridging the freedom […] or the right of the people to petition the Government*"[2]. Un primo passo in avanti, seguito presto da molti altri, si ebbe nel 1946 con

[1] Cfr. N. BOBBIO e N. MATTEUCCI, *Dizionario di Politica*, Torino, Utet, 1976.
[2] Primo emendamento della Costituzione degli Stati Uniti d'America.

l'approvazione del *Federal Regulation of Lobbying Act* che regolò severamente l'attività di "promozione degli interessi particolari", con l'obbligo da parte del lobbista di dichiarare non solo il tipo di interesse rappresentato ma anche le relative entrate ed uscite connesse alla promozione dell'interesse stesso[3]. Da una prospettiva penalistica, altrettanto severe sembrano le sanzioni previste per chi decida di non registrarsi e di fare attività di *lobbying* occultamente (si rischia fino ad un massimo di 5 anni di carcere).

Il Canada non è da meno. Secondo quanto dichiarato dall' *Office of the Commissioner of Lobbying*, sono circa 5000 i lobbisti presenti sul territorio canadese. Nel 2008 si è proceduto ad un'ulteriore modifica del *Lobbying Act* canadese, erede del *Lobbyists Registration Act* del 1989, in cui il *lobbying* viene identificato con quelle attività "portate avanti in cambio di un compenso". Al suo interno troviamo una dettagliata ed attenta definizione di lobbista, che suddivide in tre tipi la categoria: *Consultant Lobbyist, In-house Lobbyist (Corporation), In-house Lobbyist (Organization).*

A Bruxelles, dove la concentrazione di "rappresentanti di interessi" è seconda solo a Washington DC, è tutta un'altra storia. A differenza degli Stati Uniti, l'Unione Europea non ha ritenuto necessario impiegare un sistema di legislazione vincolante, preferendo di gran lunga il più moderato meccanismo di auto-regolamentazione. Nel 1996 il Parlamento Europeo decise di muoversi per l'emanazione di una serie di regole sul *lobbying* parlamentare[4], presto converse in un unico Codice di condotta. Recentemente rivisto, questo codice è stato adottato dalle associazioni europee, quali la *Society of European Public Affairs Professionals* (SEAP) e la *Public Affairs Practitioners* (PAP), che operano in "*Public Affairs*". Insieme di buone pratiche alle quali i gruppi aderiscono volontariamente, il Codice di condotta europeo richiede anzitutto una presentazione sistematica, per nome e compagnia di appartenenza. Buona parte di queste pratiche sono state riprese dal Parlamento europeo nel Codice di condotta per i gruppi di

[3] Cfr. INSTITUTE OF PUBLIC ADMINISTRATION (IPA), *Regulation of Lobbyists in Developed Countries*.
[4] *Rule of Procedure* 9, Annex I and Annex IX.

interesse, allegato al suo regolamento interno[5]. Tra le operazioni domandate, vi sono la necessaria registrazione e sottoscrizione di tutti i lobbisti che, per ottenere informazioni, si recano regolarmente al Parlamento europeo, ottenendo in questo modo un pass speciale come operatore in "*Public Affairs*" [6]. Meno severo e rigoroso di quello statunitense, il sistema di regolamentazione europeo prevede sanzioni che, a seconda della gravità del reato, vanno dalla denuncia orale al ritiro del *pass* consegnato alle persone interessate. Queste sanzioni sono estendibili anche ai professionisti che non rispettano il Codice di condotta. Gli assistenti accreditati, per evitare ciò ed esercitare liberamente le loro funzioni, devono rilasciare "una dichiarazione scritta sulle proprie attività professionali e su qualsiasi altra funzione o attività retribuita da essi esercitata".

Tornando alla definizione di lobbismo, pregnante è quella scelta dal Parlamento europeo. Con essa si indica quell'attività "intesa ad esercitare un'influenza non solo sulle decisioni politiche e legislative, ma anche sull'attribuzione dei fondi comunitari e sul controllo e l'applicazione della legislazione. Tutti i soggetti esterni alle istituzioni dell'UE corrispondenti a tale definizione dovrebbero essere considerati

[5] *Regolamento Interno Parlamento europeo*, Allegato IX, art 3: "Nel quadro delle loro relazioni col Parlamento, le persone figuranti nel registro previsto all'articolo 9, paragrafo 2 : a) devono rispettare le disposizioni dell'articolo 9 e dell'annesso presente ; b) devono dichiarare ai deputati, al loro personale o ai funzionari delle istituzioni l'interesse o gli interesse che essi rappresentano ; c) devono astenersi da ogni iniziativa col fine di ottenere informazioni disonestamente ; d) non passano riferirsi ad alcuna relazione ufficiale con il Parlamento in qualunque rapporto con terzi ; e) non possono distribuire, a fine di lucro, a terzi, delle copie di documenti ottenuti presso il Parlamento ; f) devono conformarsi strettamente alle disposizioni dell'annesso I, articolo 2, secondo comma (Disposizioni relative alla dichiarazione degli interessi finanziari dei deputati) g) devono assicurarsi che tutta l'assistenza fornita nel quadro delle disposizioni dell'annesso I, articolo 2, sia dichiarata nel registro previsto a questo scopo ; h) devono conformarsi, in caso di reclutamento di ex-funzionari delle istituzioni alle disposizioni dello statuto dei funzionari ; i) devono conformarsi a ogni regola definita dai parlamenti su diritti e responsabilità di ex-deputati ; j) per evitare eventuali conflitti di interesse, devono ottenere l'accordo preventivo del o dei deputati interessati per ciò che riguarda ogni legame contrattuale con un assistente o ogni assunzione di un assistente e assicurarsi, in seguito, che questo sia dichiarato nel registro previsto all'articolo 9, paragrafo 2."

[6] *Regolamento interno del Parlamento Europeo,* Allegato IX, Art 1.

lobbisti e trattati nello stesso modo"[7]. L'elenco è lungo, le tipologie varie: lobbisti professionisti, lobbisti aziendali "interni", ONG, centri di studi ed associazioni di categoria, sindacati ed organizzazioni dei datori di lavoro, organizzazioni aventi scopo di lucro ed organizzazioni non-profit nonché gli studi legali, "qualora il loro scopo sia di influenzare gli orientamenti politici anziché fornire assistenza legale e patrocinio in giudizio o prestare assistenza legale". A Bruxelles l'attività di *lobbying*, superando l'intermediazione degli interessi che spetterebbe alla politica, rivela la sua natura di elemento extra- politico di articolazione della democrazia, dispiegando tutta la sua potenza e la sua capacità di penetrazione nelle scelte dei *decision-makers*. L'azione lobbistica è principalmente orientata a facilitare il lavoro del funzionario europeo. In particolare, la sua funzione-obiettivo è quella di fornire con tempestività tutte le informazioni di cui possa necessitare il funzionario per svolgere bene il suo lavoro. Il *lobbying* sul Parlamento europeo, similmente a quanto avviene per il *lobbying* nel Parlamento nazionale, non deve però intendersi come minaccioso sostituto alla rappresentanza democratica, ma piuttosto come reale e concreta alternativa capace principalmente di influenzare il processo legislativo (tenendo conto soprattutto dei limitati poteri riconosciuti al Parlamento europeo).

La strada è lunga ed impervia, ma l'Europa ha finalmente deciso di percorrerla. Oggi la questione di una regolamentazione più formale dei lobbisti sta avanzando in cima all'agenda politica di tutti quei paesi che, accertata (ed accettata) l'esistenza dei gruppi di pressione, hanno intenzione di capire come regolarne le numerose attività. Il bilanciamento tra l'articolazione degli interessi delle lobby ed alcuni principi democratici fondamentali, come la libertà di espressione e di associazione all'interno del sistema di policy, si rivela un'incalzante necessità moderna che preme contro il mantenimento dello status quo voluto dalla maggioranza dei Parlamenti nazionali. Come evidenzia Margaret Mary Malone[8] nel suo studio sulla regolamentazione delle

[7] Cfr. *Risoluzione del Parlamento europeo dell'8 maggio 2008 sull'elaborazione di un quadro per le attività dei rappresentanti di interessi (lobbisti) presso le istituzioni europee (2007/2115(INI))*, in *GUUE*, C 271 E del 12 novembre 2009.
[8] Cfr. INSTITUTE OF PUBLIC ADMINISTRATION (IPA), *op. cit.*

lobby, il problema consiste nel fatto che la regolamentazione formale, fatti salvi Usa e Canada, tende ad essere ancora oggi più l'eccezione che la regola. In Europa, e non solo, l'adozione di un approccio sensibilmente meno vincolante e rigido, e pertanto più informale rispetto a quello in vigore negli *States*, è diventata la norma. Il quadro attuale di regolamentazione necessita di un regime che sia efficace e tenga conto non solo del proprio sistema di *governance* ma anche della propria cultura politica ed amministrativa. Insomma, per un'attività "pulita e sicura" ogni paese, se non lo ha già fatto, dovrà attrezzarsi del depuratore della fiducia da parte delle istituzioni e dell'opinione pubblica.

2. Perché e come le lobby possono far bene alla democrazia.

> *"Lobbyists are people who make me understand a problem in ten minutes, while my advisors take three days"*
>
> J. F. Kennedy

Il *lobbying* ha un raggio d'azione molto ampio: spazia dalla difesa di cause etiche, come l'ambiente e i diritti dei minori, agli interessi economici di grandi aziende. Il fatto che esista una pluralità di interessi rappresentati dai lobbisti, e che siano coinvolte innumerevoli categorie di attività, fa emergere una visione più netta e completa delle questioni sottese alle scelte di *governance* (e degli interessi che ne verrebbero premiati o danneggiati). Molto spesso il bravo lobbista mette le sue doti diplomatiche al servizio della costruzione del consenso verso una determinata decisione, utilizzando la tecnica molto "*soft*" del *nudging*. Districandosi abilmente tra l'ipertrofia di emendamenti, commi e clausole varie, il lobbista riesce a far convergere in un'organica e solida organizzazione gli interessi di soggetti tra loro congruenti e sinergici, tanto che possono essere considerate lobby le filiere industriali, le associazioni ed i sindacati (all'elenco si potrebbero aggiungere persino le comunità territoriali). La tutela degli interessi di categoria, obiettivo centrale dei gruppi di pressione, appare senza dubbio un elemento molto positivo ed innovativo delle comunità. Tutto sta nella costituzione di basi sicure

per la regolamentazione, in quanto l'esistenza stessa di una sorta di tracciabilità delle decisioni, che fa bene alla democrazia e alle istituzioni, è una *condicio sine qua non* per la fiducia da parte dei cittadini.

Oggi le lobby stanno dispiegando la loro forte capacità di formazione del consenso intorno ad esse, proponendosi come attori extra-politici nel quadro generale delle decisioni delle democrazie moderne, che risultano fortemente rafforzate dall'espansione della loro base di partecipazione ai gruppi d'interesse.

Riguardo all'idea di una democrazia rafforzata dalle lobby, Giuseppe Mazzei ritiene che si debbano raggiungere quattro obiettivi:
"- eguaglianza dei soggetti portatori di interessi;
- efficienza e competenza nei processi decisionali;
- autonomia ed indipendenza delle istituzioni, degli eletti e dei funzionari pubblici;
- separazione tra finanziamento della politica e il suo condizionamento.

(…) la vita politico-istituzionale risulterebbe depurata da commistioni indebite e legittimata da una migliore trasparenza"[9].

In mancanza di regolamentazione, a dominare sarebbero al contrario gli interessi delle impenetrabili consorterie di potere consolidato. Scegliere di adottare una politica "pro-emersione del sommerso", con una successiva e necessaria mediazione delle istituzioni, è la chiave di volta nel processo di regolamentazione dell'attività di *lobbying*. Se dietro la definizione di politica si nasconde nient'altro che "rappresentazione di interessi", risulta a questo punto preferibile la scelta di una manifestazione evidente di interessi ad una ammantata di interesse generale. Le lobby, sia chiaro, non sono dei soggetti alternativi, né tantomeno opposti, a quelli politico-istituzionali. La loro affermazione ed emersione, non scaraventerebbe affatto i partiti politici o le istituzioni nella caverna buia e desolata "dell'antidemocraticità". Partecipano al processo decisionale ma senza sostituirsi alla politica, aiutandola in questo modo a funzionare meglio. I poteri e le rispettive sovranità sono già

[9] Cfr. G. MAZZEI, *Lobby della trasparenza*, Roma, Centro di documentazione giornalistica, 2009.

ben delineate nel concreto meccanismo della cooperazione attiva. Abili mediatori, i lobbisti cercano di influenzare le scelte politiche, proponendo quelle richieste dei cittadini altrimenti non ascoltate.

Il ruolo ricoperto da questi soggetti extra-politici per la rappresentanza degli interessi, individuali e di gruppo, trova terreno fertile nel campo neutrale della collaborazione attiva. Non capita di rado, infatti, che le lobby svolgano anche una "funzione di supplenza" della politica. Il *lobbying* riesce a far funzionare meglio la macchina politica liberando o costruendo nuovi canali della partecipazione politica o fungendo da interlocutore tra i rappresentanti politici e cittadini. Le lobby non sono antidemocratiche e la loro azione non indebolisce minimamente la struttura democratica del paese che le riconosce e regolamenta. Con altrettanta sicurezza si può affermare anche che esse costituiscano oggi la forza vitale delle democrazie moderne. E basterebbe buttare l'occhio un po' oltre l'oceano Atlantico, soffermandosi sulla storia della politica americana, per avere una più concreta conferma del fatto che l'azione delle lobby sia direttamente proporzionata alla crescita della potenza e della forza dei governi. Articolazione della società civile contro lo strapotere dello Stato, possono concorrere alla formazione di una volontà "generale" che trova la propria espressione negli atti legislativi, governativi o amministrativi. L'attività di *lobbying* costituisce un momento di difesa di interessi dei cittadini, quegli stessi interessi che lo Stato, dotato di poteri e ambiti d'azione troppo vasti, non si prodiga a conoscere o a preferire nella sua agenda politica, sacrificandone altri. Un passo ulteriore, e decisivo, consiste nel loro riconoscimento formale da parte delle istituzioni. Le lobby trasparenti sono la linfa delle democrazie moderne, a condizione però che si riesca a stabilire un'eguaglianza di opportunità accompagnata dall'eliminazione di qualsiasi forma di legame tra lobbismo e finanziamento della politica, il più grave ostacolo all'inserimento del *lobbying* in una dimensione professionale. Dove il meccanismo è trasparente, la presenza di lobbisti professionali e organizzati può contribuire a raggiungere un livello tecnico più elevato nella discussione politica, perché ciascun lobbista è portatore di informazioni. Le crepe comunicative ed informative, esistenti tra gli effettivi decisori politici ed i cittadini, sono attenuate da un maggiore grado di neutralità decisionale

derivante dal progresso tecnologico in ambito telematico. Proprio su questo terreno si sta svolgendo la nuova partita del *cyberlobbying*, così bellamente definito da Giuseppe Mazzei. "Le lobby hanno compreso immediatamente le potenzialità della rete come mezzo a proprio vantaggio: mettere in linea le informazioni sulle questioni di pubblico interesse; illustrare le posizioni e i punti di vista; le rivendicazioni dei gruppi di pressione; l'invio di I agli iscritti alle community e non solo; informare costantemente quanti appoggiano la campagna di *lobbying* delle azioni in corso per raggiungere l'obbiettivo preposto; creare spazi di discussione e di scambi d'idee ecc… sono solo alcune delle opportunità di cui le lobby fanno uso per la propria attività"[10]. Ed è proprio grazie alla trasmissione, telematica e non solo, delle informazioni e delle richieste, nei più vasti e vari settori, che le lobby sono riuscite a ritagliarsi precocemente un loro spazio nell'arena politico-istituzionale europea.

La mescolanza di svariate culture giuridiche, spesso molto diverse tra loro, nell'ordinamento comunitario ha permesso alle lobby di gestire nel modo più opportuno gli interessi e di non soffrire di quel pregiudizio negativo che incontra in alcuni paesi, Italia in primis. Il Parlamento europeo ha riconosciuto ampiamente come l'attività di *lobbying* ricopra ormai "un ruolo essenziale nel dialogo aperto e pluralistico su cui si basa ogni sistema democratico" rappresentando "un'importante fonte d'informazione" per i deputati nell'esercizio del loro mandato. Un accesso trasparente e paritario a tutte le istituzioni europee ne costituisce la *condicio sine qua non* per la legittimità stessa dell'Unione europea. Il problema del deficit democratico resta il nervo scoperto del complessivo quadro europeo. Basta ricordare che la Commissione non è eletta, o che il Consiglio lo è solo indirettamente, per toccare con mano l'imperfezione dell'euromacchina. Per non parlare del Parlamento Europeo, in cui dovrebbero essere rappresentati gli interessi degli elettori, ma dove in realtà si riscontra una forte carenza partecipativa, un controllo democratico assente, un potere legislativo flebile e una presenza di gruppi politici ancora lontani dall'essere europei nel loro funzionamento. Ancora una volta, la soluzione al problema sono le lobby.

[10] Cfr. G. MAZZEI, *Lobby della trasparenza, op. cit.*

L'Unione europea soffre di un'insufficiente capacità operativa e la regolamentazione del *lobbying*, coerentemente con il rispetto dei principi di trasparenza e parità d' accesso all'interno del processo democratico, sembra essere una risposta concreta alla richiesta di maggiore trasparenza delle istituzioni europee e dei relativi processi decisionali. Una democrazia pluralista non è nemmeno lontanamente pensabile senza il riconoscimento di gruppi di pressione, che siano capaci di attivare meccanismi di partecipazione all'interno della società civile e tra essa e le istituzioni. Il *lobbying* gioca una partita fondamentale negli equilibri democratici, impedendo alla politica di essere l'unica detentrice delle decisioni e delle conoscenze sulla dinamica degli interessi. Debellando il germe insano dell'isolazionismo del potere politico, gestisce il flusso informativo di bisogni e domande che regola il sistema decisionale, consentendo a tutti i portatori di interesse di far sentire la propria voce. Le lobby, direttamente o indirettamente, sono la manifestazione concreta della sanità operativa e funzionale del sistema pluralistico. Sono le sinapsi informative che si creano tra politica ed istituzioni, tra istituzioni e società civile. Senza di esse, o senza una gestione trasparente delle loro attività, vi sarebbe una mancanza certa del confronto diretto con i cittadini, che tanto bene fa alla democrazia, un allontanamento delle istituzioni ed un intasamento dei complessi canali di comunicazione tra i centri di potere e la società civile. Insomma, il *lobbying* è un dato di fatto, ed uno dei vanti di ogni democrazia parlamentare è la trasparenza del suo funzionamento. Si deve tornare a dare una dignità alle lobby, ad intenderle nel vecchio, e sicuramente più appropriato, significato. Un'area centrale (interessi privati) a "cielo aperto", circondata da corridoi coperti (*decision- makers*), da cui si accede ai principali locali (interessi pubblici), o in una parola, "*lobium*".

3. Tra il dire e il fare c'è di mezzo l'Italia.

"Lobby" è una parola sporca per la maggior parte degli italiani. Come per altre parolacce, la sua sporcizia può essere ripulita tramite esposizione alla luce, cioè ripetendola più volte senza scuse né imbarazzi. Non essendo ancora riconosciuta dall'opinione pubblica

come una professione, diventare un lobbista risulta essere oggi "un desiderio strano" per un italiano, quasi una perversione. Come vuole la tradizione, a spaventare l'immaginario collettivo è la sua natura segreta o di tacito interesse privato. La caccia alle lobby è aperta e torna la tentazione del populismo puritano di fingere di non vedere lo stretto legame esistente tra interessi e decisori politici.

Il vuoto normativo e regolamentare sulla trasparenza per le lobby è il *punctum dolens* di un sistema politico-istituzionale per certi aspetti arretrato ed inadatto. Questo vuoto andrebbe colmato *hic et nunc*, inaugurando al più presto il nuovo rinascimento italiano delle lobby, attraverso una coraggiosa politica di riforme e di modernizzazione. Oltre la metà dei decisori italiani ritiene che il maggiore handicap dell'attività di *lobbying* sia il non essere sufficientemente trasparenti. Non a caso le più recenti proposte di legge presentate in Parlamento si pongono più o meno tutte nell'ambito della corruzione e dei modi per controbatterla[11]. Dal 1979 ad oggi, sono più di trenta le proposte di legge presentate alle Camere[12], ed altrettanti i fallimenti. Intanto le lobby italiane sembrano continuare ad annaspare nell'opacità.

A rattoppare i buchi dello stivale, e della legislazione italiana in materia, ci pensano però le regioni. Nel 2002 sono state approvate in Toscana le norme per regolamentare l'attività dei «gruppi di pressione[13]», con più di 115 lobby accreditate. Successivamente la Regione Molise, seguendone l'esempio, ha replicato la legge toscana con la legge regionale n. 24 del 2004. Una forte sensibilità al tema della trasparenza si è riscontrata anche in Calabria, Veneto ed Emilia Romagna dove sono state presentate altre proposte. Tutto merito dell'effetto del decentramento dei poteri a livello locale. Da Nord a

[11] Cfr. M. FOTIA, *Le lobby in Italia: gruppi di pressione e potere*, Bari, Edizioni Dedalo, 2002.

[12] La più recente è il ddl Garavaglia (PD) del 2008,"*Regolamentazione dell'attività dei Consulenti in relazioni istituzionali presso le pubbliche istituzioni*", che codifica la facoltà per imprese ed enti pubblici di avvalersi di persone e organizzazioni che svolgano l'attività di lobby, anche in forma non esclusiva, purché accreditati con le modalità in esso previste.

[13] La legge regionale non dà una definizione di gruppi di interesse né di pressione o lobby. L'art. 2 distingue due tipologie di gruppi: quelli che rappresentano categorie economiche, sociali, del terzo settore e sono maggiormente rappresentative a livello regionale e provinciale; e altri gruppi comunque attivi sul territorio toscano.

Sud, quella della trasparenza dell'attività di rappresentanza di interessi sembra essere la soluzione ottimale e condivisa per porre fine alla storica prevaricazione dei più forti sui deboli. Ma il successo non è sempre alla portata di tutti. E' dunque fondamentale creare un clima d'opinione favorevole poiché in Italia siamo solo, ed ancora, agli inizi.

L'iniziativa della trasparenza è un obiettivo comune di tutte le proposte di legge, tre delle quali depositate alla Camera ad inizio legislatura. L'intenzione delle proposte è portare i lobbisti alla luce del sole, rompere il muro del silenzio di una cultura politica che ancora mantiene un pregiudizio tanto negativo quanto infondato. Le ultime tre iniziative legislative propongono la creazione di un registro di portatori di interesse, sulla scia del rigoroso *Lobbying Act* americano o del più moderato Codice di condotta di Bruxelles.

Il lobbismo rappresenta una risposta ai molti dubbi italiani, oltre che un tentativo di rottura con l'arretratezza delle decisioni politiche e di avvicinamento tra cittadini ed istituzioni. Con esso si riesce a misurare l'efficacia delle decisioni politiche prese dai governi, ad evitare di fare scelte poco appropriate alle esigenze della società ed a resistere alle pressioni dei più forti. Tra i progetti di legge presentati, rilevante è la proposta, molto sentita ma fino ad ora poco considerata, che siano gli stessi decisori pubblici a poter chiedere l'intervento dei rappresentanti dei gruppi d'interesse nelle forme più svariate, che vanno dalle più generiche informazioni e ricerche alle memorie scritte. Piuttosto che limitarsi alla mera regolamentazione, bisognerebbe infatti puntare i riflettori sulla realizzazione di una vera e propria fase di dialogo, grazie alla quale il lobbista possa far luce su quanto espresso nella fase istruttoria del processo decisionale parlamentare. In questo modo la valutazione legislativa, che trova la sua collocazione nell'ambito della legistica, non verrebbe più esclusa dal campo di interesse del lobbista e, per estensione, di tutti coloro che operano in una democrazia moderna, dal singolo cittadino alle grandi associazioni. Fornire una migliore base informativa alla decisione legislativa, attraverso una costante verifica del conseguimento del risultato, rappresenterebbe una concreta soluzione all'allarmante fenomeno della inflazione e dell'inquinamento legislativo.

Un atteggiamento propositivo ed ottimista, volto a tutelare non soltanto i membri della categoria di appartenenza ma soprattutto gli interessi degli utenti e dei consumatori del servizio, permetterebbe inoltre alle lobby di riacquistare presso l'opinione pubblica italiana, ed anche europea, la dovuta credibilità. Il ricambio generazionale sembra essere un'ottimistica soluzione per i futuri lobbisti, rafforzati dal cambiamento culturale e dalle moderne scuole di *lobbying.*

Che si tratti di regolamentazione partecipativa o di partecipazione regolamentata, una cosa è certa: per riaccendere i motori del paese servono azione e determinazione, il pane quotidiano del lobbista.

4. Parola d'ordine? Trasparenza!

Pragmatismo, ubiquità ed esperienza diretta rendono solo potenzialmente il lobbista *pars costruens* di una democrazia veramente partecipativa, oltre che moderna e rappresentativa. L'eliminazione delle barriere all'entrata, attraverso la garanzia della trasparenza e la creazione del diritto alla partecipazione al processo decisionale governativo e parlamentare, sono necessarie per consentire alle lobby una "perfetta concorrenza" con gli effettivi detentori del potere politico.

L'Istituto Italiano per la Privacy (IIP) intende fare una virata in questa direzione, sostenendo, di fatto, la promozione del "*lobbying* diretto". Centro studi dedicato alla ricerca giuridico-economica sulla protezione e sicurezza dei dati personali, l'IIP intende proporre un codice etico- professionale cui dovrebbero far riferimento tutti coloro che operano con queste prerogative. Pur non essendo una società di *lobbying*, l'Istituto sceglie di assumere, come pratica virtuosa, una via di autodisciplina basata sui principi della legalità, della responsabilità e della correttezza. La completa tracciabilità delle informazioni garantisce, inoltre, la trasparenza di tutte le attività svolte dall'associazione, sia internamente che esternamente. I principi ed i valori fondamentali che guidano l'attività dell'IIP, quali il rispetto e la difesa dei diritti fondamentali delle persone attraverso la cultura, la consapevolezza e la maturità nel trattamento dei dati personali, saranno illustrati nel Codice Etico dell'Istituto nei capitoli successivi.

Allo scopo di confermare l'immagine di prestigio e buona reputazione, il Codice Etico si propone di orientare i comportamenti individuali e quelli degli organi collegiali, quali Consiglio di amministrazione e Consiglio dei probiviri, e di condizionare le politiche di attuazione dei principali processi di funzionamento interni all'associazione stessa.

Facendo riferimento alla promozione di un contesto culturale, espresso dalle proprie finalità istituzionali, l'associazione intende dunque cercare e creare contatti con i detentori del potere legislativo ed esecutivo, nel rispetto degli imprescindibili pre-requisiti identitari della trasparenza, del buon funzionamento e del miglioramento continuo.

Attività del Garante per la protezione dei dati personali

Marketing via e-mail: possibile inviare comunicazioni a carattere promozionale solo con il consenso - 23 settembre 2010

in *boll.* n. 119/2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato, componente, e del dott. Daniele De Paoli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

VISTO il provvedimento generale del 23 maggio 2003 sullo spamming (in www.garanteprivacy.it, doc. web n. 29840) con il quale questa Autorità ha indicato le misure da adottare per l'utilizzo dei sistemi automatizzati e l'invio di comunicazioni elettroniche, per conformarsi alla normativa sul trattamento dei dati personali;

VISTA la segnalazione di Scala Reale S.r.l. del 23 novembre 2009 con la quale è stata lamentata la ricezione indesiderata di numerose e-mail per la promozione di diverse realtà aziendali, anche dopo l'invio di apposita istanza di opposizione, che risultano essere state inviate dalla società Primi sui Motori S.p.A. (di seguito indicata come "la società");

RILEVATO che la società ha affermato che i dati della segnalante sono stati estratti da una banca dati acquistata da New Project S.r.l. che avrebbe fornito espresse garanzie in merito al rispetto della normativa sulla protezione dei dati personali, senza tuttavia allegare prova dell'acquisizione del consenso preventivo e specifico della segnalante, come si evince dalle note del 29 marzo e 25 maggio 2010;

VISTO l'art. 130, comma 2, del Codice, il quale prevede, per l'invio di messaggi promozionali mediante e-mail, il presupposto del consenso informato e specifico dell'interessato, a prescindere dalla natura, di persone fisiche o giuridiche, dei destinatari delle comunicazioni, fatto salvo solo il caso previsto al successivo comma 4 del medesimo articolo 130;

CONSIDERATO che l'invio di comunicazioni commerciali mediante e-mail effettuato dalla società senza aver fornito la predetta informativa e senza l'acquisizione del prescritto consenso configura quindi un trattamento illecito di dati (artt. 13, 23 e 130 del Codice);

VISTO che il provvedimento generale del Garante in materia di spam del 29 maggio 2003 ha chiarito che *"chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito alla comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario"*;

RILEVATO che la società ritiene, come dichiarato nella nota del 29 marzo 2010, che i messaggi presenti nelle e-mail inviate non siano da considerarsi di carattere promozionale vista l'assenza di elementi atti a qualificarli come tali (quali, ad esempio: marchi, immagini pubblicitarie e prezzi);

RITENUTO che, pur in assenza degli specifici elementi sopra menzionati, il contenuto dei messaggi inviati debba invece essere considerato di carattere promozionale contenendo, ad ogni invio, la presentazione di diverse realtà aziendali ed in virtù della evidente finalità di reperimento di nuovi clienti nonché in considerazione del fatto che il servizio offerto dalla società è dalla stessa definito "e-mail marketing" come si evince dal contratto di fornitura di servizi del 1 luglio 2009 con Coop. Cartai Modenese Soc. Coop. acquisito in sede di istruttoria e depositato in atti;

RILEVATO, infatti, che per comunicazione commerciale, come stabilito nel d.lg. 9 aprile 2003, n. 70 di attuazione della direttiva 2000/31/CE sul commercio elettronico, devono ritenersi *"tutte le forme di comunicazioni destinate, in modo diretto o indiretto, a promuovere beni, servizi o l'immagine di un'impresa, di un'organizzazione o di una persona che esercita un'attività agricola,*

commerciale, industriale, artigianale o una libera professione" (cfr. art. 2, lett. f);

RILEVATO che l'invio massivo e continuativo di e-mail non sollecitate determina, anche in ragione della particolare connotazione di invasività della comunicazione, oltre che un'illegittima intrusione nella sfera privata del destinatario, ulteriori conseguenze negative quali la sottrazione di tempo ad altre attività e l'interruzione e/o alterazione della sua attività lavorativa;

VISTO che il citato provvedimento del 29 maggio 2003 ha chiarito che *"il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi"*;

RILEVATO che non risulta che la società abbia preventivamente acquisito il necessario consenso all'invio delle proprie comunicazioni promozionali via e-mail né che, come previsto dal comma 4 dell'art. 130 del Codice, le coordinate di posta elettronica siano state fornite dall'interessata nel contesto della vendita di un prodotto o di un servizio;

RILEVATO che il trattamento di dati personali effettuato dalla società risulta avere carattere sistematico;

RITENUTO inoltre che l'art. 11, comma 2, del Codice prevede che i dati trattati in violazione della normativa in materia di protezione dei dati personali non possono essere utilizzati;

CONSIDERATO che il Garante, ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, ha il compito di vietare anche d'ufficio il trattamento illecito o non corretto dei dati o di disporne il blocco e di adottare, altresì, gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

RITENUTA conseguentemente la necessità di adottare nei confronti della società un provvedimento di divieto del trattamento illecito di dati personali ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice correlato all'invio di comunicazioni commerciali

mediante e-mail senza che risulti comprovato il necessario consenso preventivo, specifico e informato del destinatario;

RITENUTA, altresì, la necessità di adottare nei confronti della società un provvedimento prescrittivo ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice;

TENUTO CONTO che, ai sensi dell'art. 170 del Codice, chiunque, essendovi tenuto, non osserva il presente provvedimento di divieto è punito con la reclusione da tre mesi a due anni e che, ai sensi dell'art. 162, comma 2-ter, del Codice, in caso di inosservanza del medesimo provvedimento, è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila a centottantamila euro;

RISERVATA, con autonomo procedimento, la verifica dei presupposti per contestare le violazioni amministrative concernenti l'omesso rilascio dell'informativa e l'omessa acquisizione del consenso (artt. 13, comma 4, 161, 23, 130, comma 2, e 162, comma 2-bis, del Codice);

RILEVATO, altresì, che resta impregiudicata la facoltà per l'interessata di far valere i propri diritti in sede civile in relazione alla condotta accertata (cfr. anche art. 15 del Codice), con specifico riguardo agli eventuali profili di danno;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

Relatore il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE:

a) dichiara illecito il trattamento dei dati personali effettuato da Primi sui Motori S.p.A., con sede legale in Modena, viale Finzi, 587, tramite l'invio di e-mail promozionali indesiderate;

b) ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, vieta alla società Primi sui Motori S.p.A. il trattamento di qualunque dato personale effettuato tramite l'utilizzo della e-mail per l'invio di comunicazioni promozionali a terzi senza che risulti la prova documentata di aver acquisito il consenso preventivo, specifico e informato degli interessati ai sensi dell'art. 130 del Codice;

c) invita la società Primi sui Motori S.p.A. ad adottare tutte le misure necessarie e opportune atte a garantire la completa ottemperanza a quanto stabilito nella precedente lettera b), fornendone adeguata documentazione al Garante entro trenta giorni dalla notificazione del presente provvedimento.

Roma, 23 settembre 2010

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
De Paoli

Comunicazioni "captate" su reti wi-fi: il Garante ordina a Google Street View il blocco dei dati e trasmette gli atti alla magistratura - 9 settembre 2010

in *boll.* n. 119/2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

VISTE le note del 27 aprile e del 14 maggio 2010 inviate da Google Italy S.r.l., con le quali l'Autorità è stata informata che Google Inc., durante il passaggio nel territorio italiano delle vetture che acquisivano immagini per il servizio Street View, ha raccolto sia dati relativi alla presenza di reti Wi-Fi (*wireless fidelity*) sia frammenti di comunicazioni elettroniche trasmesse dagli utenti su alcune reti Wi-Fi non protette da protocolli sicuri e da cifratura (*c.d. payload data*);

VISTA la nota di questa Autorità del 17 maggio 2010, con la quale è stato comunicato l'avvio di un procedimento amministrativo nei confronti di Google, teso alla verifica della liceità e correttezza dei trattamenti ed avente ad oggetto l'osservanza delle disposizioni in materia di protezione dei dati personali nell'ambito del servizio Street View;

CONSIDERATO che, con la medesima nota, l'Autorità ha chiesto alla predetta società di fornire elementi utili alla valutazione complessiva dei trattamenti dei dati personali effettuati tramite il richiamato servizio Street View, invitando contestualmente la società a non effettuare alcun ulteriore trattamento dei *payload data* fino a diversa direttiva del Garante;

VISTA la nota del 1° giugno 2010, con la quale Google Inc., elettivamente domiciliata presso lo Studio legale Hogan Lovells in

Roma, ha fornito i primi riscontri in relazione alla raccolta dei dati relativi alla presenza di reti Wi-Fi e ha confermato di aver raccolto, a partire dal mese di aprile 2008, *payload data* durante il passaggio delle vetture di Street View nel territorio italiano utilizzando antenne Wi-Fi e appositi software;

CONSIDERATO che la società ha dichiarato di ritenere che i *payload data* siano estremamente frammentati, dal momento che *"le vetture Google Street View sono costantemente in movimento e l'impianto WiFi cambia automaticamente canale cinque volte al secondo"*, ma che *"sussiste la teorica possibilità che i payload data contengano dati personali nel caso in cui un utente, al momento della raccolta, abbia trasmesso alcune informazioni personali"*;

CONSIDERATO che, secondo le dichiarazioni della società, tali dati sono stati raccolti erroneamente, non sono mai stati utilizzati per alcun tipo di servizio, non sono mai stati comunicati a terzi e attualmente sono conservati su server localizzati negli Stati Uniti, in una banca dati separata ad accesso limitato ai soli soggetti appositamente incaricati da Google Inc. per la protezione dei dati;

CONSIDERATO che Google Inc. ha raccolto i *payload data* per un considerevole periodo di tempo (aprile 2008 - maggio 2010), in modo sistematico e nell'ambito di un'attività svolta su tutto il territorio nazionale e che, quindi, vi è la concreta possibilità che alcune fra le informazioni raccolte abbiano natura di dati personali;

RITENUTO che all’eventuale trattamento di dati personali posto in essere, in quanto effettuato mediante strumenti situati nel territorio dello Stato, si applichino le norme del Codice (art. 5 del Codice);

VISTO l’art. 11, comma 1, lett. *a*) e *b*) del Codice, ai sensi del quale i dati personali devono essere trattati in modo lecito e secondo correttezza e devono essere raccolti e registrati per scopi determinati, espliciti e legittimi;

VISTO l’art. 15 della Costituzione che sancisce l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione e che stabilisce che *"la loro limitazione può avvenire*

soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge";

VISTO l'art. 617-*quater*, comma 1, del codice penale, che punisce *"chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi (…)"*;

VISTO l'art. 617-*quinquies*, comma 1, del codice penale, che punisce *"chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire od interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi (…)"*;

RITENUTO, sulla base degli elementi acquisiti nel corso dell'istruttoria, che il trattamento realizzato da Google Inc., per quanto concerne in particolare i *payload data*, possa porsi in contrasto con le richiamate norme del codice penale e che pertanto debba essere disposta la trasmissione degli atti del presente procedimento all'Autorità giudiziaria per le valutazioni di competenza;

CONSIDERATO che l'art. 11, comma 2, del Codice prevede che i dati personali trattati in violazione della disciplina rilevante in materia di dati personali non possono essere utilizzati;

RITENUTA la necessità che i *payload data* raccolti non vengano per il momento cancellati dai server sui quali sono conservati, in quanto gli stessi potrebbero costituire elementi di prova in caso di un eventuale intervento da parte dell'Autorità giudiziaria;

CONSIDERATO che il Garante, ai sensi degli artt. 143, comma 1, lett. *c*) e 154, comma 1, lett. *d*), del Codice, ha il compito di disporre il blocco anche d'ufficio del trattamento illecito o non corretto dei dati e di adottare, altresì, gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

RILEVATA pertanto la necessità di adottare nei confronti di Google Inc. un provvedimento di blocco del trattamento ritenuto illecito ai sensi dell'art. 154, comma 1, lett. *d*), del Codice correlato alla raccolta di *payload data* effettuata durante il passaggio delle vetture di Street View nel territorio italiano;

TENUTO CONTO che, ai sensi dell'art. 170 del Codice chiunque, essendovi tenuto, non osserva il presente provvedimento di blocco è punito con la reclusione da tre mesi a due anni e che, ai sensi dell'art. 162, comma 2-*ter* del Codice, in caso di inosservanza del medesimo provvedimento, è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro;

RISERVATO ogni ulteriore accertamento e intervento in merito al trattamento di dati relativi alla presenza di reti Wi-Fi effettuato da Google Inc. e all'acquisizione di immagini per il servizio Street View, profili rispetto ai quali è tuttora in corso l'istruttoria dell'Autorità;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

TUTTO CIÒ PREMESSO IL GARANTE:

A) dispone nei confronti di Google Inc., ai sensi degli artt. 143, comma 1, lett. *c*) e 154, comma 1, lett. *d*), del Codice, il blocco di qualsiasi trattamento dei *payload data* raccolti sul territorio italiano.

B) dispone la trasmissione di copia degli atti del procedimento e del presente provvedimento all'Autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili.

Roma, 9 settembre 2010

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
De Paoli

Rigetto dell'istanza di autorizzazione riguardante l'esonero dell'informativa da rendere agli interessati con riguardo al trattamento di dati presenti nel database telefonico unico (DBU) - 16 settembre 2010

in *boll.* n. 119/2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan, del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

VISTA l'istanza di Consodata S.p.A. (di seguito "Consodata") del 13 aprile 2010 con la quale la società ha richiesto l'esonero, ai sensi dell'art. 13, comma 5, lett. c) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice") dell'informativa da rendere agli interessati con riguardo al trattamento di dati presenti nel database telefonico unico (cd. DBU), costituito ai sensi della delibera n. 36/02/Cons e della delibera n. 180/02/Cons dell'Autorità per le garanzie nelle comunicazioni, di seguito "DBU";

VISTO il provvedimento del Garante del 23 maggio 2002 con il quale l'Autorità ha segnalato a tutti gli operatori le garanzie necessarie per trattare dati personali al fine di formare i nuovi elenchi telefonici e prestare i servizi di informazione agli utenti;

VISTO il provvedimento del Garante del 15 luglio 2004 con il quale l'Autorità ha prescritto a tutti gli operatori le misure ancora da adottare, le garanzie e le modalità per il trattamento dei dati personali relativi agli elenchi telefonici comunque realizzati e la fornitura dei servizi di informazione all'utenza;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO:

Consodata S.p.A. ha presentato a questa Autorità, in data 13 aprile 2010, un'istanza per "esonero/semplificazione dell'informativa per manifesta sproporzione ai sensi dell'art. 13. 5, lett. c) del Codice" tra l'impiego dei mezzi necessari per l'adempimento dell'onere del rilascio dell'informativa ai soggetti presenti nel DBU ed il diritto tutelato.
La società ha motivato la suddetta istanza evidenziando di voler acquisire i dati presenti nel DBU per trasferirli nel proprio database telefonico al fine di cederli successivamente in licenza d'uso alla propria clientela. Detti dati sarebbero trattati da Consodata, in qualità di autonomo titolare, e ceduti a soggetti terzi (anch'essi autonomi titolari) per la realizzazione di finalità diverse da quelle di promozione commerciale o di ricerca di mercato e non richiederebbero l'acquisizione del consenso dei soggetti interessati, essendo in particolare volti a realizzare finalità proprie di soggetti pubblici, ovvero particolari finalità di soggetti privati che peraltro non esporrebbero a rischi meritevoli di considerazione i diritti tutelati dalla normativa in materia di protezione dei dati personali.

La richiesta di "esonero/semplificazione" dell'informativa da rendere in forma individuale è stata motivata dalla circostanza che i dati presenti nel DBU riguarderebbero milioni di utenti tra aziende ed individui e che anche il rilascio di un'informativa ai nuovi abbonati che progressivamente entrano a far parte di tale database comporterebbe un'attività estremamente complessa. La società dovrebbe pertanto affrontare notevoli difficoltà organizzative ed economiche per informare in modo adeguato un numero particolarmente elevato di soggetti.

Nell'istanza la società ha quindi proposto modalità alternative per consentire agli abbonati di essere comunque informati degli elementi di cui al citato art. 13 del Codice.

CONSIDERATO CHE:

- la disposizione applicabile nell'ipotesi evidenziata dalla società istante non concerne la semplificazione dell'informativa (art. 13,

comma 3, del Codice), quanto piuttosto l'esonero o le modalità equipollenti per informare gli interessati rispetto a dati personali acquisiti da terzi (art. 13, commi 4 e 5, del Codice), posto che Consodata dovrebbe acquisire i dati presso terzi estraendoli in particolare dal DBU telefonico;

- l'art. 13, comma 5, lett. c), del Codice prevede l' "esonero" dall'obbligo dell'informativa diretta, orale o scritta, all'interessato rispetto ai dati personali raccolti presso terzi, qualora l'informativa stessa comporti un impiego di mezzi che il Garante dichiari manifestamente sproporzionato rispetto al diritto tutelato;

- le finalità del trattamento dei dati personali presenti nel DBU rappresentate da Consodata non risultano previste tra quelle per le quali tale banca dati unica è stata costituita;

- in base alle citate delibere n. 36/02/Cons e 180/02/Cons dell'Autorità per le garanzie nelle comunicazioni, nonché ai provvedimenti del Garante del 23 maggio 2002 e 15 luglio 2004, il DBU rappresenta, infatti, un archivio elettronico unico che raccoglie i dati personali dei clienti di tutti gli operatori di telefonia fissa e mobile (compresi i possessori di carte prepagate) per la formazione dei nuovi elenchi telefonici e la fornitura dei servizi di informazione abbonati;

- come esplicitato inoltre nel modello di informativa diretta all'abbonato (All. IV al provvedimento di questa Autorità del 15 luglio 2004) il DBU costituisce un *"… archivio elettronico unico (…) dove sono presenti anche i dati di tutti gli operatori di telefonia fissa e mobile, che li possono consultare ed utilizzare al solo fine di prestare i servizi (…) richiesti…"* dall'abbonato, *"…realizzare gli elenchi telefonici, prestare servizi di informazione ed eventualmente inviare pubblicità, promozioni, offerte commerciali, ecc…"* se richiesti dall'abbonato stesso;

- ogni trattamento dei dati presenti nel DBU per finalità diverse da quelle per le quali detto database è stato costituito vìola, pertanto, il principio di finalità di cui all'art. 11, comma 1, lett. *b*) del Codice e rende il trattamento illecito ed il dato inutilizzabile ai sensi del successivo comma 2 della norma.

TUTTO CIÒ PREMESSO IL GARANTE:

rigetta l'istanza con cui Consodata S.p.A. ai sensi dell'art. 13, comma 5, lett. *c*) del Codice in materia di protezione dei dati personali ha richiesto l'esonero dall'informativa con riguardo al trattamento dei dati personali dell'abbonato presenti nel database telefonico unico (cd. DBU) per finalità diverse da quelle per le quali detto archivio elettronico è stato costituito, configurandosi tale trattamento di per sé illecito ai sensi dell'art. 11, comma 1, lett. *b*) del Codice.

Roma, 16 settembre 2010

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
De Paoli

Google Street View: le auto dovranno essere riconoscibili - 15 ottobre 2010

in *boll.* n. 120/2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

VISTA la nota del 18 settembre 2008 con la quale Google Inc. ha comunicato all'Autorità l'intenzione di rendere operativo in Italia il servizio *Street View*, fornendo, contestualmente, informazioni in merito allo stesso e chiarendo che esso *"consente agli utenti di visualizzare le foto panoramiche delle strade di una città italiana dove il servizio è attivo"* e che è possibile *"fare lo zoom della foto, spostarsi con il mouse del P.C. avanti ed indietro lungo le strade e persino ruotare la visuale di 360°"*;

VISTA la nota di Google Inc. del 1 giugno 2010, con la quale la società, elettivamente domiciliata presso lo studio legale Hogan Lovells in Roma, ha fornito all'Autorità ulteriori elementi in merito al servizio *Street View*;

CONSIDERATO che, secondo quanto dichiarato dalla società, le immagini sono riprese, al livello della strada, da particolari fotocamere posizionate su veicoli in grado di scattare fotografie in movimento e che, a seguito della loro acquisizione, le stesse sono inviate automaticamente al *server* di Google Inc. negli Stati Uniti dove si provvede all'elaborazione ed all'inserimento delle foto selezionate sul sito *web* di Google, mediante il quale sono oggetto di diffusione *online* per diversi mesi;

CONSIDERATO che, in alcuni casi, le predette fotografie contengono anche dati personali, quali, ad esempio, immagini di individui o targhe di veicoli;

VISTE le numerose segnalazioni pervenute a questa Autorità, relative proprio all'acquisizione di immagini da parte della società che, nel fotografare i luoghi, ha ripreso anche soggetti identificabili che non desideravano comparire sulle fotografie pubblicate *online* da Google;

CONSIDERATO che il servizio *Street View*, in ragione delle sue caratteristiche, nonché sulla base degli elementi emersi dall'analisi delle predette segnalazioni, rende necessaria una riflessione più ampia sul rispetto dei principi in materia di protezione dei dati personali;

RITENUTO che al trattamento di dati personali posto in essere da Google Inc. si applichino le norme del Codice, in quanto effettuato mediante strumenti situati nel territorio dello Stato (art. 5 del Codice);

RITENUTA, quindi, la necessità che Google Inc., in qualità di titolare del trattamento, provveda a designare un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali;

CONSIDERATO che al caso in esame risulta applicabile la disciplina relativa all'uso delle immagini e che quindi, in linea generale, non è necessario acquisire il consenso degli interessati quando la ripresa fotografica avviene in luogo pubblico, salve le limitazioni previste dalla legge, quali, ad esempio, il divieto di diffusione di fotografie quando ciò comporti pregiudizio all'onore, alla reputazione, al decoro della persona ripresa (art. 97, comma 2, della l. 22 aprile 1941, n. 633) o il divieto di diffusione di dati idonei a rivelare lo stato di salute (art. 26, comma 5 del Codice);

CONSIDERATE, tuttavia, le peculiari caratteristiche delle fotografie scattate da Google Inc., che, oltre ad essere oggetto di diffusione *online* per un considerevole periodo di tempo, possono essere ingrandite per consentire all'utente una visualizzazione dettagliata delle stesse;

CONSIDERATO che, comunque, il trattamento di dati personali svolto da Google Inc. per la fornitura del servizio Street View deve

avvenire nel rispetto dei principi di liceità, proporzionalità, correttezza e necessità sanciti dall'art. 11 del Codice;

RITENUTO, che, al riguardo, risulta opportuna la misura già adottata da Google Inc. di oscurare, prima della pubblicazione *online*, gli elementi che possono consentire un'identificazione diretta (ad esempio, i volti) o indiretta (ad esempio, le targhe dei veicoli) degli interessati;

CONSIDERATO che resta fermo – ai sensi dell'art. 7 del Codice – il diritto di opposizione degli interessati rispetto ai dati personali che li riguardano, e che, in tal senso, la società già assicura agli interessati l'esercizio di tale diritto, mediante una particolare procedura di "segnalazione" *online*;

CONSIDERATO che Google Inc. deve garantire l'effettivo esercizio dei diritti di cui all'art. 7 anche quando, nonostante la procedura di oscuramento posta in essere, gli interessati siano comunque, anche se solo indirettamente, riconoscibili;

RITENUTO che risulta necessario, comunque, che gli interessati siano informati in modo idoneo ai sensi dell'art. 13 del Codice in relazione all'acquisizione di immagini da parte di Google Inc., affinché costoro possano scegliere di sottrarsi alla "cattura" delle immagini, allontanandosi dal luogo oggetto di ripresa;

CONSIDERATO che le modalità con le quali attualmente è fornita l'informativa agli interessati, in relazione al trattamento di acquisizione delle immagini, risultano del tutto insufficienti, in quanto consistono nella sola pubblicazione, sul sito *web* della società, dell'indicazione generica delle città in cui transitano le vetture di *Street View*, alcune ore prima del loro passaggio, nonché di un testo contenente alcune informazioni sul servizio *Street View* che tuttavia non soddisfa pienamente i requisiti di cui all'art. 13 del Codice;

CONSIDERATO, tuttavia, che il rilascio dell'informativa a ciascun interessato oggetto di riprese da parte di Google Inc. comporterebbe un impiego di mezzi obiettivamente sproporzionati rispetto al diritto tutelato;

CONSIDERATO che il Garante, per effetto dell'art. 13, comma 3, del Codice, può prescrivere al titolare del trattamento l'adozione di misure semplificate per fornire un'idonea informativa agli interessati;

RITENUTA, pertanto, l'opportunità di adottare nei confronti di Google Inc. un provvedimento prescrittivo ai sensi degli artt. 143, comma 1, lett. *b*) e 154, comma 1, lett. *c*) del Codice;

RILEVATA la necessità che Google Inc. informi gli interessati, in relazione all'acquisizione di immagini fotografiche, individuando con un sufficiente livello di approssimazione le località visitate dalle vetture di *Street View* tenendo conto della ampiezza delle suddette località (ad esempio per le grandi città è necessario indicare i quartieri in cui circoleranno le vetture). Ciò, mediante pubblicazione della notizia sul sito *web* della società, nei tre giorni antecedenti rispetto all'inizio della raccolta delle immagini;

RILEVATA, altresì, la necessità che Google Inc. fornisca idonea e preventiva informativa anche tramite la pubblicazione, sulla pagina di cronaca locale di almeno due quotidiani, di un avviso – per ogni regione visitata - che informi sui luoghi in cui circoleranno le vetture;

RILEVATA la necessità che analogo avviso preventivo sia diffuso anche per il mezzo di almeno un'emittente radiofonica locale;

RILEVATA, altresì, la necessità che Google Inc. predisponga, sulle vetture con le quali acquisisce le immagini fotografiche, cartelli o adesivi ben visibili che indichino, in modo inequivocabile, che si stanno acquisendo immagini fotografiche istantanee oggetto di pubblicazione *online* mediante il servizio *Street View*;

CONSIDERATO che resta comunque ferma la necessità che Google Inc. renda un'informativa completa di tutti gli elementi indicati dall'art. 13 del Codice, disponibile sul sito *web* della società;

TENUTO CONTO che, ai sensi dell'art. 162, comma 2-ter del Codice, in caso di inosservanza del presente provvedimento prescrittivo è applicata in sede amministrativa la sanzione del pagamento di una somma da trentamila euro a centottantamila euro;

RISERVATO ogni ulteriore accertamento e intervento in merito ad ulteriori profili relativi all'acquisizione di immagini per il servizio *Street View*;

RISERVATA, con autonomo procedimento, la verifica dei presupposti per contestare la violazione amministrativa concernente l'inidoneità dell'informativa resa da Google Inc. (artt. 13 e 161 del Codice);

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

TUTTO CIÒ PREMESSO IL GARANTE:

dispone, ai sensi degli artt. 143, comma 1. lett. *b*) e 154, comma 1, lett. *c*) del Codice, che Google Inc. entro trenta giorni dalla notificazione del presente provvedimento:

a) provveda a designare un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali;

b) provveda ad informare gli interessati, relativamente all'acquisizione di immagini fotografiche, individuando con un sufficiente livello di approssimazione le località visitate dalle vetture di *Street View* tenendo conto della ampiezza delle suddette località, mediante pubblicazione della notizia sul sito *web* della società, nei tre giorni antecedenti rispetto all'inizio della raccolta delle immagini;

c) provveda ad informare gli interessati anche tramite la pubblicazione, sulla pagina di cronaca locale di almeno due quotidiani, nonché mediante diffusione per mezzo di un'emittente radiofonica locale, di un preventivo avviso – per ogni regione visitata – che informi sui luoghi in cui circoleranno le vetture;

d) predisponga, sulle vetture attraverso le quali acquisisce le immagini fotografiche, cartelli o adesivi ben visibili che indichino, in modo inequivocabile, che si stanno acquisendo immagini fotografiche

istantanee oggetto di pubblicazione *online* mediante il servizio *Street View*.

Roma, 15 ottobre 2010

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
De Paoli

Finito di stampare nel mese di dicembre 2010

Contributi

- ***Alessandro Del Ninno***
  La privacy nel mercato europeo delle comunicazioni elettroniche: cosa cambia dopo la direttiva 2009/136/CE di riforma della direttiva 2002/58/CE sulla tutela dei dati personali nel settore delle comunicazioni elettroniche

- ***Elena Finotti***
  Tecnologie DRM e TPM per la protezione delle opere e implicazioni sulla privacy degli utenti finali

- ***Nicola Fabiano***
  La privacy sta cambiando? Dalle privacy-enhancing technologies (PETs) alla privacy by design (PbD)

- ***Paolo Balboni***
  Google, Street View, and Privacy: An Objective Look from Europe

- ***Michele Iaselli***
  Intercettazioni telefoniche e telematiche: un giusto equilibrio tra privacy, giustizia ed informazione

- ***Stefano Mele***
  Privacy ed equilibri strategici nel cyber-spazio

- ***Giovanni Crea***
  Il trattamento dei dati personali nell'analisi del comportamento del consumatore

- ***Antonella Romano***
  Il Lobbying "legistico-giuridico": un'attività da centro studi del terzo millennio

Attività del Garante per la protezione dei dati personali

- Marketing via e-mail: possibile inviare comunicazioni a carattere promozionale solo con il consenso - 23 settembre 2010

- Comunicazioni "captate" su reti wi-fi: il Garante ordina a Google Street View il blocco dei dati e trasmette gli atti alla magistratura - 9 settembre 2010

- Rigetto dell'istanza di autorizzazione riguardante l'esonero dell'informativa da rendere agli interessati con riguardo al trattamento di dati presenti nel database telefonico unico (DBU) - 16 settembre 2010

- Google Street View: le auto dovranno essere riconoscibili - 15 ottobre 2010