

e-Privacy 2008

UGO PAGALLO

(Università degli studi di Torino)

Zio Sam e i ventisette nani?

*Dall'accordo PNR tra USA e UE ai nodi
della privacy nella società della "nuova
sorveglianza"*

Firenze, 10 maggio

Sommario

1. Introduzione: “**incomprensioni**”
2. “**Convergenze**”: gli accordi PNR
3. La società della “**nuova sorveglianza**”
4. Conclusioni: sulle nuove **frontiere tecnologiche** degli ordinamenti (giuridici) contemporanei

(1). Incomprensioni

Nel tenere corsi di privacy sia negli USA (Georgetown) sia nell'UE (Torino, Londra) mi capita di assistere non di rado a significativi *misunderstandings*...

Mi limito a evidenziarne due, peraltro particolarmente emblematici

Visioni americane

The perspective is different in other countries, Rosen said. Americans are, in general, concerned with **preventing terrorism**, while Europeans are concerned with **protecting** their individual **privacy**, he said. For example, the French will bare their breasts but not their salaries and mortgages, and **the reverse is true in the US**. "My fear is that the cultural differences will make thoughtful regulation difficult," Rosen said.

(Jeffrey Rosen, George Washington University, riportato da CNET News.com, 10.03.2008)

Visioni europee

“...negli Stati Uniti, che non hanno conosciuto l’esperienza dei regimi totalitari, non deve stupirci che **lo Stato non sia chiamato a proteggere i dati personali**”

(Giulia TIBERI, *Riservatezza e protezione dei dati personali*, in *I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, a cura di M. Cartabia, Il Mulino, Bologna 2007, p. 354)

(2). Convergenze

Per una volta pregiudizi (e scarsa conoscenza delle fonti) sembrano essere stati superati nel valutare gli accordi tra USA e UE/CE sul cosiddetto regime PNR (i.e., ***Passenger Name Record***): vediamone innanzitutto il background

Background

- ▶ CGE causa C-317/04 e C-318/04 (decise il 30 maggio 2006)
- ▶ Cambio di competenza: dalla Comunità all'Unione europea
- ▶ Nuovo accordo PNR (6 ottobre 2006)
- ▶ Nuovo accordo PNR (23 luglio 2007)
- ▶ Scadenza prevista: luglio 2014

10 punti critici

Riprendendo la risoluzione del **Parlamento europeo** del 12 luglio 2007, mettiamo a fuoco almeno dieci punti critici (e criticabilissimi) dell'accordo

I. Mancanza di controllo democratico

La trattativa è stata condotta e conclusa senza alcun coinvolgimento del Parlamento europeo e senza alcuna opportunità per i parlamenti nazionali di esercitare qualche influenza sul negoziato

II. Mancanza di certezza giuridica

Molte delle clausole dell'accordo fanno temere per il principio di certezza del diritto, in quanto il DHS americano tratta i dati (europei) secondo le leggi USA e, soprattutto, in base agli impegni che il DHS dichiara di assumere nella lettera DHS allegata agli accordi (v. punto (3) dell'accordo PNR)

III. Vaghezza degli scopi

Oltre al terrorismo e altri seri crimini, l'accordo fa riferimento a una non ben precisata "protezione degli interessi vitali della persona interessata o di altre persone" (v. la terza ipotesi contemplata nel primo punto della lettera di Michael Chertoff a Luis Amado)

IV. Trasparenza

Nonostante gli impegni al riguardo (punto 7 dell'accordo PNR e 6 della lettera Chertoff) l'esperienza quotidiana dei viaggiatori tra le due sponde dell'Oceano dimostra quanta “greater visibility” e “public information” vi sia a proposito del funzionamento dei sistemi PNR e il relativo trattamento dei dati personali

V. Livello di tutela

L'accordo PNR tra USA e UE sembra obiettivamente offrire minori garanzie rispetto ad analoghi accordi UE con l'Australia e il Canada:

PROBLEMA DELLE FONTI

DURATA DEL TRATTAMENTO

NUMERO DI DATI

(...)

VI. Paesi terzi

Nella stessa clausola (6) dell'accordo PNR in cui il DHS s'impegna a garantire un adeguato livello di tutela dei dati trattati, l'Europa s'impegna a "non interferire nei rapporti tra gli USA e paesi terzi nello scambio d'informazioni sui passeggeri per via della protezione dei dati" !!!

VII. Data retention

Il punto (VII) della lettera di Chertoff, chiarito che il DHS riterrà i dati PNR per 7 anni in un database “analitico attivo” e per 8 in uno “dormiente”, fa sapere che l’ipotesi di distruggere quei dati trascorsi i 15 anni sarà “parte di future discussioni” !!!

VIII. Profiling & Data Mining

Non è difficile essere d'accordo con il Parlamento europeo quando sottolinea i rischi sottesi al regime di data retention concordato tra USA e UE:

Rispetto ai rischi di profiling e data mining denunciati dal Parlamento, è significativo che l'accordo PNR non preveda in alcun modo la supervisione delle autorità garanti europee per il trattamento dei dati !!!

IX. Push & Pull Systems

Ancora oggi (maggio 2008) permangono dubbi e incertezze sulla transizione tra i due sistemi: dal prelevamento diretto dei dati da parte delle autorità americane alla trasmissione da parte dei vettori europei (v. clausole 2 e 3 dell'accordo)

X. Retroattività

Per finire, last but not least, la lettera di Chertoff dichiara a conclusione del punto (VII) che le modalità di trattamento dei dati previste dall'accordo "si applicano anche ai dati raccolti sulla base dei precedenti accordi tra USA e UE del 28 maggio 2004 e 19 ottobre 2006" !!!

Problemi aperti

- ▶ L'accordo PNR tra UE e USA va inteso nel più ampio quadro definito dai temi della lotta al terrorismo e della globalizzazione
- ▶ Un esempio concreto: l'accordo tra USA e Germania del maggio 2007 (cui faccio solo un cenno, dato che l'accordo deve essere ancora formalmente ratificato dal Parlamento tedesco)

Tendenze in atto

L'accordo USA-Germania dell'11 maggio 2007 prevede, ad esempio, all'art. 12, la messa a disposizione, oltre che del Dna, anche dei dati dei cittadini riguardanti «razza o provenienza etnica, opinioni politiche, religiose, convinzioni di altra natura o l'appartenenza sindacale»

(3). La nuova sorveglianza

Come riferito, l'intento è di considerare l'accordo PNR tra USA e UE nel **più vasto quadro** definito da temi e motivi della cosiddetta società della "**nuova sorveglianza**": ai problemi sorti con la lotta al terrorismo e la globalizzazione, vanno così aggiunti quelli proposti dall'uso delle **nuove tecnologie**

Attualità del tema: 2 convegni

3rd [Surveillance & Society](#)

Conference, Sheffield 2008

InVisibilities: The Politics, Practice and Experience of Surveillance in Everyday Life

*A two-day international
conference hosted by
the Centre for Criminological
Research, University of
Sheffield
in association with the
Surveillance Studies Network*

Legal Futures Conference

**March 8, 2008 from 9:00 am -
4:00 pm**

**Google and Stanford Law
School's Center for Internet
and Society:** A conversation
between some of the world's
leading thinkers about the
future of privacy, intellectual
property, competition,
innovation, globalization, and
other areas of the law
undergoing rapid change due
to technological advancement.

Cronaca di una morte annunciata?

Fin dal principio (1890) l'istituto giuridico della privacy è venuto intrecciandosi al **progresso della tecnica**: in particolare, le prime “candid photographs” dell'Eastman Kodak Co. nel 1884 !!!

Di qui, al giorno d'oggi, il proliferare di **dichiarazioni di morte** presunta...

Paradise Lost?



**“You have zero
privacy now.
Get over it!”**

(Scott McNealy, CEO
Sun Microsystems)

Diritto e Tecnica

Alla base della popolarità di tesi come quelle di *The End of Privacy* (Sykes, 1999), *Database Nation* di Jarfinkel (2000), o *Privacy Lost* di Holtzmann (2007), c'è certamente il fatto che la tecnologia contribuisce a ridefinire i termini del problema. Illustriamo il punto con la tesi di Gary Marx in *What's New About the "New Surveillance"? Classifying for Change and Continuity* ("Surveillance and Society", 2002, 1, 1, pp. 9-29)

Vecchia e nuova sorveglianza

Mentre, **precedentemente**, il sorvegliante cercava di scoprire cose che erano ovviamente a conoscenza del sorvegliato, **oggi**, viceversa, il sorvegliante viene spesso a conoscenza di dati personali del sorvegliato che, tuttavia, lo stesso interessato non conosce (e.g., DNA)

Discontinuità

Muta radicalmente il **senso** in cui si afferma, oggi, di “osservare”, “seguire con attenzione” o “tenere sotto controllo” qualcuno o qualcosa:

1. Automatizzazione dei processi di controllo
2. Raccolta dati continua e onnipresente, immanente all'azione quotidiana
3. Disponibilità in tempo reale

Alcuni esempi

1. Sensori di calore, luce, suono, movimento e olfatto (→ Aml: Ambienti Intelligenti)
2. Dispositivi sorveglianza video/audio
3. Strumenti di accesso biometrico
4. RFIDs
5. Sistemi esperti di analisi/reperimento dati
6. Satelliti
7. Visori notturni

L'impatto tecnologico

Il modo in cui muta il senso del vedere e del sorvegliare può essere riassunto con 4 coppie di concetti con cui la privacy è stata spesso associata:

- ▶ Esterno / Interno
- ▶ Visibile / Invisibile
- ▶ Pubblico / Privato
- ▶ Incluso / Escluso

Esterno / Interno

Privacy tradizionale

Lo spazio fisico della casa come “castello di ogni uomo”
(Warren-Brandeis e la tradizione delle garanzie di cui, ad esempio, al **IV emendamento**)

Privacy digitale

Raccolta e trattamento dei dati **immanenti** alla vita quotidiana, **sfumando** la distinzione tra **fuori** (e.g., CCTV) e **dentro** (cookies e spyware in casa!)

Visibile / Invisibile

Privacy tradizionale

Lo “**stato di solitudine**”
di Warren/Brandeis
aggiornato con la
mancaza
d'**informazioni** su un
soggetto determinato
(v. Ruth Garrison)

Privacy digitale

L'**integrale visibilità**
che si accompagna
all'invisibilità della
automazione
tecnologica solleva il
problema (politico) del
controllo sui dati

Publico / Privato

Privacy tradizionale

L'identificazione tra privacy e **segretezza** e l'idea che si tratti di una zona in cui l'**accesso** all'informazione personale è ristretto o **limitato**

Privacy digitale

La **privatizzazione** delle indagini penali va di pari passo con l'**uso pubblico** di dati commerciali, mentre **muta il senso** personale del dato (e.g., profiling e data mining di **161 milioni di giga** nel solo 2006!!!)

Incluso / Escluso

Privacy tradizionale

La possibilità di **escludere** gli altri, diventando “del tutto inaccessibili” (Warren/Brandeis) o rimanendo in uno “stato di **solitudine**” (Alan F. Westin)

Privacy digitale

La necessità di **non essere inclusi** nel processo onnipervasivo di raccolta, trattamento ed estrazione d'**informazione** a mezzo dati (digitali)

(4). Le nuove frontiere

La tecnologia permette di **vedere cose** che prima semplicemente non era possibile vedere, in **modo continuo** e onnipresente, **immanente** alla vita quotidiana, disponibile in **tempo reale**, ampliando spettro e **profondità** dei dati trattati, anche al fine di **anticipare il futuro!**

Qualche obiezione al determinismo

Mi limito a enunciarne tre:

- a) Le tecnologie liberalizzanti (Amitai Etzioni)
- b) Le radici culturali della privacy
- c) Motivi politici

Tecniche a fin di bene

Non si tratta d'insistere sulla presunta
“neutralità” del mezzo quanto di rimarcare
le stesse possibilità aperte dai dispositivi e
ricavati tecnologici:

L'emblematico caso dei *digital recommender
systems* di nuova generazione
(si v. il ricordato convegno di Sheffield)

Cultura e Privacy

Più che dall'inesorabile evoluzione della tecnologia, le sorti della privacy sembrano dipendere dal **clima di disinteresse, indifferenza e trascuratezza** denunciato anche dagli organizzatori di e-privacy 2008: mi limito a segnalare che, da oltre dieci anni, s'insegna *computer ethics* nelle scuole elementari (!) giapponesi

Motivi politici

Proprio perché la rivoluzione tecnologica in corso **non** decreta di per sé la **morte della privacy** – ma obbliga a ripensare i nuovi termini in cui si profila la tutela della persona umana e dei suoi diritti fondamentali nella società dell'informazione – **occorre denunciare** gli accordi e i provvedimenti di legge adottati in questi ultimi anni che, obiettivamente, stanno compromettendo il **necessario bilanciamento** tra privacy e sicurezza di cui all'art. 8 CEDU

Ritorno all'inizio dell'analisi

In sostanza, nell'inquadrare i problemi sollevati dall'accordo PNR del 2007 tra USA e UE nel più vasto quadro proposto dai temi della nuova sorveglianza, occorre sottolineare come le sfide che essa pone, passino attraverso la denuncia di accordi come quello che ho esaminato e promuovendo la sensibilità di un'opinione pubblica fin qui, per lo più, distratta o assente