

E Privacy 2003

Firenze, Palazzo Vecchio 14 giugno 2003

***Il trattamento dei dati personali
nel corso delle indagini
preliminari nel processo penale
ordinario e penale minorile***

**Avv. Barbara Gualtieri - Foro di Firenze
www.craiat.it Università degli Studi di Firenze
www.strano.net**

La tutela costituzionale dei dati esterni alla comunicazione

Tabulato di traffico – ovvero manifestazioni visibili della realtà costituita dai dati esterni di una comunicazione

Interesse per il dati esterni – riferimenti locali; riferimenti temporali (conversazione telefonica); analisi incrociata dei dati

Differenza con i dati di contenuto – oggetto; modo per apprenderli

Allarmismi giuridici

Sono dati veramente esterni alla comunicazione?

Potenzialità e capacità di rappresentare una persona – informazioni sulle sue conoscenze; sui suoi movimenti

Che tipo di protezione prevede o deve prevedere l'ordinamento giuridico per queste modalità di controllo delle comunicazioni ?

Quali forme deve prevedere l'azione giudiziaria?

La Costituzione e la Corte Costituzionale

Sentenza n°81 del 11 marzo 1993 – Giur. Cost. 1993 p.731 – Questi dati possono trovare copertura costituzionale sub art. 15 – La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per *atto motivato dell’Autorità giudiziaria* e con *le garanzie stabilite dalla legge*.

Interpretazione innovativa che supera la mera garanzia per il solo contenuto

Sviluppo per la prima volta del concetto di “spazio vitale” antecedente dell’attuale concetto di privacy – la segretezza della comunicazione è una manifestazione dello spazio vitale di una persona ovvero della sua privacy

Prospettive dell'art. 15 Costituzione

Doppia forma di tutela

- soggettiva: provvedimento dell'Autorità giudiziaria;
- oggettiva: riserva di Legge

Qual è la norma di riferimento per l'apprensione dei tabulati di traffico ? – l'art. 256 c.p.p. - 1. *Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato [202, 204] ovvero di segreto inerente al loro ufficio o professione [103 comma 2] (1).*- Prevede la possibilità di invitare soggetti detentori di documentazione che rivestano un “ruolo pubblico di rilievo” ad esibirla. Quindi non tutela il comunicante ma il soggetto che detiene la documentazione, che sarebbe tenuto al riserbo se non intervenisse il provvedimento della A.G.

Perplessità sull'art. 256 c.p.p.

Necessità di una normativa che disciplini casi e modi in cui la prova a mezzo tabulati può formarsi – per assicurare il livello di garanzia richiesto dalla Corte Costituzionale

Incostituzionalità dell'art. 256 c.p.p. ? - una tale pronuncia avrebbe effetti paralizzanti in concreto, considerato che i tabulati costituiscono oggi uno strumento basilare di indagine

Riserva di Legge inattuata – mancanza di un presupposto indefettibile dell'utilizzabilità della prova; rischio di un sindacato di costituzionalità diffuso estraneo al nostro ordinamento

La tutela ordinaria

I dati esterni alla comunicazione appartengono alla sfera privata

- I diritti afferenti la sfera privata trovano il loro riconoscimento costituzionale non nell'art. 15 ma nell'art. 2
- Una delle direzioni in cui si manifesta la sfera privata "privacy" è la manifestazione del pensiero
- La fonte legislativa del trattamento dei dati esterni alla comunicazione è la Legge sulla privacy n° 675/96 e successive modificazioni, art. 21 / 4: la condizione richiesta è che vengano osservate le norme che regolano la materia

Quadro conclusivo

Scomparsa della riserva di legge

Scomparsa della riserva di giurisdizione

La strada che parte dell'art. 15 Cost. sembra l'unica adatta ad interpretare lo spirito dei tempi

L'atto comunicativo ha una pregnanza di senso e un livello di espressività che non hanno altre manifestazioni personali. La possibilità di essere gestito da soggetti estranei attraverso accumuli cognitivi lo rende particolarmente e pericolosamente sensibile. Appare indispensabile una Legge regolatrice dell'acquisizione dei dati esterni che disciplini casi, modi e garanzie. In tal senso l'art. 8 Convenzione europea per la salvaguardia dei diritti dell'uomo richiede la previsione di Legge per le ingerenze dell'Autorità Pubblica nella vita privata – caso *Malone vs. Regno Unito*.

Sicurezza e controllo dati negli U.S.A. dopo l'11 settembre ...

Modifiche sostanziali della disciplina legislativa in materia di mezzi di prova elettronica – legislazione antiterrorismo U.S.A. Patriot Act

Distinzione

- esame delle informazioni che riguardano il futuro e raccolta di informazioni in tempo reale “sorveglianza e intercettazione”
- analisi dati storici precedentemente immagazzinati “mail inviate ricevute e lette”

Elementi di prova

- in ordine al contenuto “alto grado di tutela”
- estranei al contenuto “basso grado di tutela”

Electronic Communication Privacy Act – U.S.A. (1)

Adottato negli anni 80' con l'avvento delle nuove tecnologie informatiche

Acquisizione in tempo reale di informazioni **non** attinenti al contenuto

- l'accusa certifica alla Corte che le informazioni che verranno presumibilmente attengono ad una investigazione in corso

- dopo l'11 settembre, il mandato può essere emesso in ogni località degli U.S.A. che abbia una relazione del caso non solo dal distretto in cui si sarebbe eseguito il monitoraggio

Electronic Communication Privacy Act – U.S.A. (2)

Acquisizione in tempo reale di informazioni attinenti al contenuto

- l'accusa richiede alla Corte un mandato sulla base del titolo 3 "parte della Legge che disciplina le intercettazioni telefoniche"
- requisiti rigorosi per i contenuti di fonia e per le comunicazioni elettroniche:
 - motivazione valida
 - approvazione del dipartimento di Giustizia centrale
 - certificazione che altri sistemi sono stati tentati ma sono falliti
 - termine perentorio per la richiesta "30 giorni"
 - limite della "minimizzazione per informazioni non pertinenti"
- dopo l'11 settembre, è stata introdotta "l'eccezione del violatore di computer" ovvero può essere monitorato il violatore di computer che accede senza autorizzazione o con l'autorizzazione scaduta poiché si ritiene che egli non abbia una ragionevole aspettativa di riservatezza

Altre forme di acquisizione

Distinzione tra provider “privati” - “datore di lavoro” che fornisce account ai dipendenti senza fornire servizi al pubblico e **provider “pubblici”** – AOL, MSN, EARTHLINK

I “privati” nella maggior parte dei casi **possono** fornire informazioni “indirizzi IP, registrazione di transazioni, modalità” alle Autorità che svolgono le indagini senza ordine della Corte; i “pubblici” **non possono** dare le informazioni senza il consenso del cliente.

Dopo l’11 settembre – un provider può consegnare spontaneamente i dati all’Autorità se ritiene la sussistenza di un pericolo immediato alla “sicurezza nazionale”

Differenti standard di dati archiviati (1)

Messaggi elettronici non letti dal destinatario, nella casella di posta da meno di sei mesi – “alto grado di tutela”

Messaggi elettronici letti o non letti ma nella casella di posta da oltre sei mesi - “basso grado di tutela”

Il Congresso nell’approvare la Legge ha ritenuto che se l’interessato dopo aver letto la posta non l’ha cancellata entro sei mesi non è presumibilmente interessato alla riservatezza, così come se il messaggio è rimasto nella casella per sei mesi e nessuno lo ha letto.

Differenti standard di dati archiviati (2)

Report di flussi telematici “orario di invio, dimensione messaggio, destinatari, mittenti” – ordine relativo ai fatti articolabili, cd ordine D. L'accusa produce alla Corte, che spesso ben disposta ad approvarli, dei fatti che mostrino come quei dati costituiscano prove da correlare ad una indagine in corso

Lett. F – è lo strumento che viene utilizzato dagli inquirenti per richiedere al provider di conservare qualunque elemento di prova in suo possesso relativo ad un particolare account o utente per un periodo di 90 giorni. Trattasi di una semplice lettera che può essere faxata o assumere la forma di una comunicazione telefonica.

Tutela dei minori

Tecniche di indagine in ordine alla pedopornografia online

Legge 3 agosto 1998 n°269 – ha introdotto nuovi reati integrando il Capo III dei delitti contro la personalità individuale aggiungendo dopo l'art. 600 c.p. gli articoli dal 600 bis al 600 quinquies

600 ter c.p.

- **[III]**. Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni ...

Tutela dei minori

600 ter c.p.

- [IV]. Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, **consapevolmente** cede al altri, anche a titolo gratuito, materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto, è punito con la reclusione fino a tre anni ...

Difficoltà di natura investigativa e processuale

- **capacità** degli organi di P.G. di individuare siti, chat, newsgroup, mail in cui avviene lo scambio;
- **particolare competenza** per l'attività di contrasto affidata dall'art. 14 L.268/98 al Questore o al Comandante provinciale dei C.C. e della G.d.F per il compimento di attività simulata, previa autorizzazione motivata da parte dell' A.G.

**Attività da svolgersi sotto copertura
“ispirata dall’esperienza maturata
nella lotta al traffico degli stupefacenti”**

- Acquisti simulati di materiale pedopornografico;
- Attività di intermediazione;
- Partecipazione ad attività a carattere turistico-sessuale;
- Apertura “siti civetta” – sito trappola /maschera di deterrenza;
- Gestione aree di comunicazione;

Attività sotto copertura con sistemi informatici

Il legislatore ha affidato solo ed esclusivamente al servizio di Polizia Postale il compito di svolgere attività sotto copertura in via telematica.

I motivi sono:

- necessità di personale altamente specializzato;
- necessità di centralizzazione e coordinamento delle attività per averne un più incisivo controllo;
- necessità di costante monitoraggio di tutte le notizie di reato attinenti a siti pedopornografici;
- la funzione di coordinamento è affidata alla direzione centrale della Polizia Criminale – Servizio centrale operativo con sede centrale a Roma e sedi periferiche sull'intero territorio.

De iure condendo

Ad oggi non esiste una visione unitaria circa le modalità con cui il P.M. deve acquisire i dati essenziali per le indagini telematiche – sarebbe opportuno prevedere una disciplina in ordine all'acquisizione di prove e dati nel corso delle indagini, nonché una disciplina specifica in materia di custodia dei file di log, affinché il corretto esito delle indagini non venga lasciato al buon senso di chi le esegue.