Senato della Repubblica XVI LEGISLATURA

N. 1759

DISEGNO DI LEGGE

d'iniziativa dei senatori PERDUCA e PORETTI

COMUNICATO ALLA PRESIDENZA IL 6 SETTEMBRE 2009

Norme in materia di raccolta, uso, conservazione e cancellazione di dati georeferenziati o cronoreferenziati, contenenti identificatori univoci di utente, effettuati mediante apparecchiature automatiche

TIPOGRAFIA DEL SENATO (490)

ONOREVOLI SENATORI. – Il presente disegno di legge per la regolamentazione dell'uso, della conservazione e della cancellazione di dati georeferenziati e cronoreferenziati raccolti con mezzi automatici e contenenti identificativi univoci di utente è stata elaborata da un gruppo di lavoro, denominato «Progetto Winston Smith», animato da Gianni Bianchini, Marco A. Calamari e Andrea Glorioso. Winston Smith, protagonista del celeberrimo romanzo di George Orwell «1984» è il simbolo dell'uomo che, pur dopo una coraggiosa opposizione, si vede costretto a soccombere al sistema del «Grande Fratello», l'oscuro e onnipotente occhio che controlla il mondo. La sua figura è stata quindi scelta per testimoniare i pericoli insiti nell'ormai dilagante espansione della rete informatica che, insieme ad indubbi e fondamentali benefici, porta con sé, però, anche la violazione della *privacy* di ogni individuo e, in definitiva, la compressione del suo spazio di libertà individuale.

La relazione che segue è tratta dal convegno «*E-privacy* 2005» tenutosi a Firenze il 27-28 maggio 2005 a cura dei citati creatori del Progetto Winston Smith. Le successive edizioni di *E-privacy*, nel 2006 e nel 2007, hanno approfondito i problemi di minacce alla *privacy*, controllo sociale e tecnocontrollo.

«Oggi è il domani di cui dovevamo preoccuparci ieri.

Visto che si parlerà di legge, vogliamo iniziare parafrasando un avvocato (e non uno qualsiasi ma Lawrence Lessig) che cominciò la sua rivoluzionaria conferenza *Architecting Innovation* parafrasando a sua volta *Guerre Stellari*: "Noi veniamo dal Lato Oscuro (...) siamo ingegneri!".

Data retention e *privacy*.

Parlare esaurientemente dei molteplici aspetti legati alla *privacy* nell'ambito delle nuove tecnologie in un breve intervento come questo sarebbe impossibile.

Anche la *data retention*, cioè la conservazione per tempi indeterminati dei dati raccolti con mezzi elettronici, è un argomento tecnico complesso; ci accontenteremo quindi di riassumerlo con degli esempi.

Nel mondo digitale.

Nel *cyberspazio*, su *Internet*, tutte le attività sono tracciate per "*default*".

Tutto quello che non è tracciato per legge o scelta commerciale è in ogni modo tracciabile e memorizzabile permanentemente in maniera tecnicamente fattibile ed economicamente realizzabile.

Collegamenti ai *provider*, dati di navigazione su *web*, *mail*, *news* e *chat* sono registrabili su scala globale già con i mezzi attuali da piccole e medie organizzazioni.

Non lo fanno solo i poteri forti, Stati o multinazionali.

Raccolta automatica di dati – GSM.

Un esempio noto ormai a tutti è quello dei cosiddetti «dati di cella» delle reti cellulari GSM.

I dati di cella sono l'elenco delle celle a cui un telefono cellulare si collega, ordinato nel tempo, continuamente aggiornato e memorizzato permanentemente su *cd-rom.*

I dati di cella sono un dettaglio tecnico nato per motivi tecnici.

La loro conservazione è una decisione tecnica del singolo gestore.

La conservazione su supporti durevoli e per periodi lunghi è (in Italia) una richiesta di legge (codice sulle comunicazioni elettroniche), generata da legittime opportunità di indagini di polizia.

La creazione di vasti *database* di questi dati è un incubo per la *privacy*: se tra dieci anni qualcuno vorrà sapere chi era presente oggi in questa sala (posto che la cosa interessi mai a qualcuno) lo potrà fare semplicemente interrogando questo *database.*

Raccolta automatica di dati – *file* di *log*.

Log dei *server web* (HTTP) 66.196.90.79 [28/Feb/2005:14:51:43 +0000] «GET /pipermail/copywhat/2004April/000561.html HTTP/1.0» – 304 «–» «mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)».

Log dei *server* di posta elettronica (SMTP).

Log dei fornitori di accesso *Internet* su linea commutata o a larga banda.

File registro di altro tipo.

Raccolta automatica di dati – RFID.

Identificazione remota a radiofrequenza di oggetti.

Evoluzione del codice a barre.

Logistica di magazzino.

Centri di distribuzione.

Controllo degli accessi.

Difficoltà di individuazione/disattivazione.

Possibilità di interrogazione *rogue.*

Identificativi univoci.

Le tecnologie citate impiegano codici che identificano univocamente un oggetto, un prodotto o un utente (UUID):

codice IMEI (GSM);
identificativo dell'etichetta (RFID).

Oppure un nodo di una rete:

indirizzo IP *(server internet*).

I dati raccolti automaticamente, inoltre, recano spesso marcature temporali o geografiche.

Risultato: identificabilità, tracciabilità, profilabilità.

«Perversione naturale».

Senza una spinta contraria, i dati proliferano, diventano immortali, possono diffondersi senza controllo.

Nessuno ha il dovere di cancellarli.

Molti hanno l'interesse a conservarli, sia perchè "non si sa mai" che per interessi commerciali; i dati sono soldi.

Tutti spingono da una parte, (quasi) nessuno spinge dall'altra.

L'equilibrio tra necessità sociali ed interessi commerciali da una parte e diritti individuali dall'altra non esiste.

La partita dei diritti dell'individuo è persa senza giocare.

Tecnocontrollo.

Il digitale, nella forma attuale, è la nemesi dell'oblio e della *privacy.* Tutto è tracciato fin dall'inizio, già oltre i più sfrenati sogni del Grande Fratello di 1984.

Nel dopoguerra Orwell non era riuscito nemmeno ad avvicinarsi al livello di tracciabilità che oggi si pratica; da soli, i dati di cella delle reti GSM, memorizzati permanentemente per legge e consuetudine, tracciano come posizione 24 ore al giorno la maggior parte di noi.

Questo senza che nessuno abbia concepito queste cose come mezzo di tecnocontrollo; sono solo un sottoprodotto delle moderne tecnologie.

Il panorama legislativo.

Nell'ordinamento americano un equilibrio tra diritti individuali e necessità sociali è garantito *(common law*) direttamente dall'inter-

pretazione della carta costituzionale da parte dei magistrati e dai precedenti. Questo rende la tutela dei diritti civili molto sensibile ai fatti di attualità; caso eclatante, il *post* 11/9.

In Italia, dove il diritto è dato dall'applicazione diretta delle leggi e poco dai precedenti, la situazione è più statica, ma la tendenza *post* 11/9 è identica; solo la velocità è diversa, ma il fine è lo stesso.

Sui termini della conservazione dei dati esistono solo due cenni in leggi recentissime (codice delle comunicazioni elettroniche, decreto legislativo n. 259 del 2003, testo unico sulla *privacy*, decreto legislativo n. 196 del 2003) e l'impianto esistente deriva principalmente da vecchi regolamenti di polizia.

Le necessità sociali e gli interessi economici tendono per loro natura a limitare le libertà individuali, quali la *privacy* e la libertà di espressione.

Autorità garanti.

A livello dell'Unione europea ed italiano esiste l'istituto dei Garanti della *privacy,* che teoricamente dovrebbe equilibrare queste spinte.

La realtà, vedi il caso italiano, è che un istituto del genere, competente ed impegnato al massimo nel raggiungimento del suo obiettivo, non ha materialmente, come organici, risorse e procedure, la possibilità di equilibrare quantitativamente le spinte degli altri poteri.

"Una bella è calda coperta, purtroppo sempre troppo corta".

Ingegnerizzazione di una soluzione legale.

Leggi digitali?

Per regolamentare la rete servono leggi speciali, leggi "digitali"? Dal nostro punto di vista, il meno possibile. Servono leggi che regolamentino i dati in sé.

Molti dei problemi concreti possono adeguatamente essere affrontati applicando le norme esistenti.

I navigatori della rete sono persone fisicamente soggette alla legge, responsabili delle proprie azioni per legge.

Internet è universale, transnazionale e non territoriale.

Le leggi possono (e debbono) regolamentare gli impatti del mondo digitale su quello fisico; nessuno realmente può (e «filosoficamente» nessuno dovrebbe) colonizzare e controllare il nuovo mondo digitale.

Una vera «legge digitale».

Quello che manca è una normativa che inizi a controbilanciare il dovere di conservare i dati, introducendo, in positivo, quello che già è enunciato a livello di principio dal testo unico sulla *privacy*, il dovere di non conservare banche dati lesive della *privacy.*

Insomma, il dovere di cancellare i dati raccolti in forma automatica.

Una proposta di legge siffatta è, almeno nel quadro legislativo italiano, assolutamente nuova (per non dire rivoluzionaria).

Non esistono leggi che sanciscano obblighi di cancellazione dei dati.

La proposta di legge del PWS (Progetto Winston Smith).

Il PWS ha cercato di ingegnerizzare una proposta di legge il più possibile compatta e minimale:

semplicità;

integrabilità nel testo unico sulla *privacy* in vigore;

economicità: stessi ruoli, procedure, responsabilità e sanzioni previsti nel testo unico;

facile applicabilità da parte di ISP, gestori telefonici, eccetera;

definizione (nel regolamento attuativo) di norme tecniche relative a casi *standard* per limitare il costo sociale.

I punti fondamentali.

Definizione di un periodo massimo di conservazione dei dati compatibile con le esigenze amministrative e tecniche.

Obbligatorietà della cancellazione dei dati alla scadenza dei termini di conservazione.

Divieto, salvo casi regolati, di conservazione dei dati per scopi diversi da quelli per cui sono stati raccolti.

Possibilità di deroga previa comunicazione all'Autorità garante.

Definizione di situazioni *standard* non soggette a comunicazione.

Assegnazione di ruoli e responsabilità alle figure già definite dal testo unico.

Cancellare i dati dovrebbe essere la regola, non l'eccezione.

Conclusioni.

Oggi, in rete, la partita della *privacy* si gioca solo ad un livello individuale, di autodifesa ma soprattutto di consapevolezza; esistono anche efficaci mezzi tecnologici ma sono poco diffusi, complessi, e quasi nessuno li usa.

Domani (forse) leggi più pragmatiche, omogenee e rispettose del Nuovo Mondo, potranno riaffermare i diritti individuali, particolarmente quelli legati alla *privacy* anche nel *Cyberspazio.*

Il Progetto Winston Smith:

http://www.winstonsmith.info E – Privacy 2005: http://e-privacy.firenze.linux.it».

DISEGNO DI LEGGE

Art. 1.

(Definizioni)

1. Ai fini della presente legge, si intende per:

a) «programma per elaboratore» *(software)* ogni programma per elaboratore elettronico, costituito da un sistema operativo o da un programma applicativo;

b) «apparecchiatura di raccolta automatica di dati personali» qualunque apparecchio fisico o programma per elaboratore che memorizza o trasmette automaticamente, in maniera temporanea o permanente, dati concernenti il proprio funzionamento o quello di altri apparecchi e programmi per elaboratore, in cui si possono potenzialmente trovare o ricavare informazioni personali o sensibili, come individuate ai sensi del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Tra le apparecchiature di raccolta automatica dei dati personali sono compresi le reti *Global System for Mobile* (GSM), i dispositivi *Radio Frequency Identification* (RFID), i *server World Wide Web* ed i sistemi di videocontrollo, nonché tutte le apparecchiature che memorizzano su *file* di *log* o su supporti analogici informazioni prodotte dall'attività di individui, quali messaggi brevi di testo, posizioni dei terminali GSM, pagine *web* accedute, luoghi e tempi di presenza, dati biometrici. Tutte le raccolte di dati riguardanti l'attività di individui che sono georeferenziate, ovvero che contengono dati di posizione geografica, o cronoreferenziate, ovvero che contengono dati di posizione nel tempo, e che contengono un identificatore univoco di un utente (IUU) appartengono alla categoria definita dalla presente lettera;

c) «gestore di raccolte di dati automatizzate» il titolare del trattamento di dati, individuato ai sensi del citato codice di cui al decreto legislativo 30 giugno 2003, n. 196, o, in sua mancanza, il responsabile organizzativo delle apparecchiature di raccolta dei dati o, in sua mancanza, il responsabile operativo delle apparecchiature di raccolta di dati;

d) «raccolta di dati personali automatizzata» qualunque archivio o flusso di dati generato da una apparecchiatura di raccolta automatica di dati personali;

e) «*file* di *log*» qualunque raccolta di informazioni effettuata da un apparecchio fisico o da un programma per elaboratore che sia utile o necessaria per il suo funzionamento, ma non ne realizzi la funzione principale;

f) «flusso di dati generato da una apparecchiatura di raccolta automatica di dati personali» la trasmissione di dati realizzata da una apparecchiatura di raccolta automatica di dati personali ad altre apparecchiature o soggetti che possono potenzialmente elaborarli o memorizzarli;

g) «procedura di *backup*» l'insieme di procedure gestionali, di elaboratori, di periferiche per elaboratori e di supporti per la memorizzazione dei dati che vengono utilizzati per garantire la conservazione temporanea di copie degli archivi di dati, al fine di consentire l'archiviazione o il ripristino dei dati stessi in caso di necessità;

h) «profilazione degli utenti» qualunque operazione che, elaborando dati provenienti da una raccolta automatizzata di dati personali, produce dati derivati che evidenziano o raccolgono informazioni sugli utenti e sui loro comportamenti riconducibili a una singola persona;

i) «identificatore univoco di un utente» (IUU) qualunque dato che permette di raggruppare e di attribuire a un singolo utente, non identificabile anagraficamente, una serie di dati, non necessariamente personali o sensibili, precedentemente raccolti in forma anonima;

l) «identificazione di un utente» qualunque operazione di elaborazione o incrocio di raccolte automatizzate di dati personali tra loro o con altri tipi di dati che può portare, anche tramite l'impiego di IUU, all'identificazione anagrafica di un utente come persona fisica.

Art. 2.

(Obblighi per i gestori di raccolte di dati automatizzate)

1. Le raccolte di dati personali automatizzate possono essere realizzate solo per consentire, controllare o agevolare il funzionamento di apparecchiature di rilevamento, di elaboratori o di programmi per elaboratore. Le raccolte di dati personali automatizzate non possono essere utilizzate per scopi diversi da quelli per cui sono state effettuate, salvo quanto disposto dal comma 2. Le raccolte di dati personali automatizzate possono essere conservate solo per il tempo minimo necessario per il motivo tecnico per cui sono effettuate e devono successivamente essere cancellate, in maniera documentabile, dai supporti originali e da tutte le copie generate da eventuali operazioni di *backup.* Per la conservazione delle raccolte di dati personali automatizzate si applicano le disposizioni del citato codice di cui al decreto legislativo 30 giugno 2003, n. 196.

2. Il gestore di raccolte di dati automatizzate che intenda elaborare i dati raccolti per scopi diversi da quelli tecnici previsti deve operare sui dati stessi considerandoli informazioni personali o sensibili, ai sensi del citato codice di cui al decreto legislativo 30 giugno 2003, n. 196, a seconda del tipo di informazioni personali che possono esservi contenute, e adempiendo agli obblighi previsti dal medesimo codice per tali tipologie di informazioni.

3. Il gestore di raccolte di dati automatizzate che intende o deve procedere a elabora-

zioni o a memorizzazioni che eccedono quelle previste dal comma 1 è tenuto a darne comunicazione a Garante per la protezione dei dati personali. Il gestore di raccolte di dati automatizzate è tenuto altresì a rendere noti la raccolta, le sue modalità, i fini e le procedure di conservazione, copia e cancellazione dei dati al citato Garante e a tutti i soggetti i cui dati possono potenzialmente essere raccolti. Le modalità di comunicazione e di determinazione dei soggetti interessati sono stabilite dal regolamento di attuazione di cui all'articolo 4, che individua anche le tipologie di elaborazione per le quali è escluso l'obbligo di comunicazione al citato Garante.

4. Ove non diversamente previsto dalla legislazione vigente in materia, il periodo massimo di conservazione di dati ricavati tramite raccolta automatizzata di dati personali o di dati derivati da essi è stabilito in tre mesi.

5. Qualora il gestore di raccolte di dati automatizzate non provveda alla cancellazione dei medesimi dati entro i termini stabiliti, ovvero li elabori o li conservi oltre il periodo stabilito o li trasmetta a terzi, è soggetto alle sanzioni previste dal citato codice di cui al decreto legislativo 30 giugno 2003, n. 196, per la stessa tipologia di violazione.

Art. 3.

(Accesso a raccolte di dati personali automatizzate da parte della magistratura e dell'autorità di pubblica sicurezza)

1. A richiesta del giudice competente o dell'autorità di pubblica sicurezza dallo stesso delegata, nell'ambito di indagini correlate a procedimenti penali pendenti o in fase di istruzione, il gestore di raccolte di dati automatizzate è tenuto a fornire i dati provenienti da raccolte di dati personali automatizzate per i soli scopi previsti dalla richiesta.

2. Con il regolamento di attuazione di cui all'articolo 4 sono individuate particolari raccolte di dati personali automatizzate di cui è prevista la conservazione per periodi di tempo inferiori a quanto disposto dall'articolo 2, comma 4. Il medesimo regolamento individua, altresì, le procedure di conservazione e di cancellazione dei dati e le procedure per la richiesta di essi da parte delle autorità competenti.

3. È comunque esclusa la possibilità di richiedere consegne generalizzate di dati che prevedono o possono portare alla creazione di banche di dati personali riguardanti interi gruppi di persone fisiche o giuridiche che non sono oggetto di indagine giudiziaria nel loro complesso. Le consegne devono essere strettamente limitate ai soli dati necessari ai procedimenti o alle indagini ed essere conservate solo per il periodo strettamente necessario.

4. I dati trasmessi al giudice competente o all'autorità di pubblica sicurezza ai sensi del presente articolo devono essere utilizzati per i soli scopi per i quali sono stati richiesti. Al termine dell'impiego, tutte le copie dei dati devono essere cancellate, fatte salve quelle eventualmente necessarie per atti obbligatori per legge. In quest'ultimo caso i dati devono essere trattati ed eventualmente resi pubblici con le stesse modalità degli atti con cui sono stati richiesti.

Art. 4.

(Regolamento di attuazione)

1. Entro sei mesi dalla data di entrata in vigore della presente legge, il Governo adotta, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, e successive modificazioni, il regolamento di attuazione della presente legge.

€ 1,00