



Berna, 12 dicembre 2008

# Protezione dei dati concernenti l'utilizzazione dell'infrastruttura elettronica della Confederazione

## Spiegazioni relative all'avamprogetto di revisione della LOGA

---

### 1 In generale

#### 1.1 Situazione iniziale

L'utilizzazione dell'infrastruttura elettronica della Confederazione (telefoni, computer, controlli degli accessi, registrazioni video ecc.) lascia inevitabilmente tracce elettroniche. Di norma non vengono memorizzati i contenuti, bensì soltanto i cosiddetti *dati marginali*, generati dall'attivazione e dalla disattivazione di collegamenti elettronici (p. es. orari e utenti di un collegamento telefonico o siti Internet visitati e i computer impiegati). Tuttavia, anche tali dati possono essere analizzati in riferimento a persone e comprendere dati personali degni di particolare protezione. L'analisi dei dati permette in alcuni casi l'allestimento di profili della personalità.

Il 20 ottobre 2005 l'Ufficio federale di giustizia (UFG), su incarico del Dipartimento federale di giustizia e polizia (DFGP), ha redatto una perizia sugli aspetti giuridici legati alla conservazione dei dati relativi alle comunicazioni, nella quale conclude che anche la conservazione (memorizzazione) dei dati marginali delle comunicazioni costituisce una forma di trattamento di dati personali ai sensi della legge federale del 19 giugno 1992 sulla protezione dei dati (art. 17 LPD; RS 235.1) e necessita quindi di una *base legale formale*, di cui gli organi federali attualmente non dispongono. In altre parole, il presente avamprogetto di revisione è inteso a fornire la base legale formale per il trattamento di dati, che in parte viene già eseguito.

In seguito a tale perizia, la Conferenza dei segretari generali si è espressa a favore di una base legale formale; il 12 novembre 2006 il DFGP ha incaricato l'UFG della preparazione di un avamprogetto. I lavori sono stati seguiti e realizzati in collaborazione con un gruppo di lavoro interdipartimentale comprendente rappresentanti della Cancelleria federale, dell'Ufficio federale dell'informatica e della telecomunicazione, dell'Ufficio federale del personale, dell'Organo strategia informatica della Confederazione e dell'Incaricato federale della protezione dei dati e della trasparenza.

#### 1.2 Progetto e punti essenziali

Le disposizioni sulla protezione dei dati qui proposte sono intese a disciplinare il trattamento dei dati connesso all'utilizzazione dell'infrastruttura elettronica della Confederazione, con due *obiettivi*: da un lato è necessario proteggere gli utenti di tale infrastruttura da un trattamento

dei dati illecito da parte dei gestori; dall'altro questi ultimi devono disporre di una base legale che li legittimi a trattare determinati dati qualora sia ritenuto necessario. Si tratta soprattutto della registrazione dei dati marginali menzionati, che tuttavia sono in parte collegati al relativo contenuto, a sua volta registrato.

Le nuove disposizioni sulla protezione dei dati non devono essere emanate in un atto normativo indipendente, ma vanno integrate in una legge esistente. Entrano in linea di conto in particolare la legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS 235.1), la legge del 24 marzo 2000 sul personale federale (LPers; RS 172.220.1) e la legge del 21 marzo 1997 sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS 172.010).

In base alla sua struttura attuale, la LPD è considerata una legge *generale*. Limitandone il campo d'applicazione agli organi federali in qualità di gestori dell'infrastruttura elettronica della Confederazione, come previsto dalle disposizioni proposte, se ne altererebbe la natura: per questo motivo rinunciamo a proporre una revisione della LPD. La LPers riguarda il personale della Confederazione. L'infrastruttura elettronica della Confederazione è utilizzata principalmente, ma non esclusivamente, dagli impiegati federali: ne beneficiano anche numerosi utenti esterni (p. es. esperti, visitatori, militari, autorità cantonali). Per questo motivo, anche la LPers è ritenuta poco adatta ad accogliere le nuove disposizioni. Alla luce di tali considerazioni, la LOGA sembra l'atto normativo più appropriato allo scopo. Infatti il campo d'applicazione è relativamente ampio: tale legge comprende già una disposizione sulla protezione dei dati in una questione connessa, ovvero il trattamento dei dati nell'ambito della gestione degli affari da parte degli «organi federali» (art. 57a<sup>1</sup>). Proponiamo pertanto un'integrazione della LOGA che faccia seguito all'articolo menzionato.

L'avamprogetto prevede anzitutto la possibilità per gli organi federali (o per l'istituzione da loro incaricata della gestione) di registrare in una prima fase praticamente tutti i dati generati dall'utilizzazione dell'infrastruttura elettronica della Confederazione. In base al principio della proporzionalità (art. 4 LPD) sarebbe necessario ammettere soltanto la registrazione di dati per gli scopi previsti e non di tutti i dati in generale, evitando quindi la raccolta di dati «a titolo di scorta». L'articolo 4 capoverso 3 LPD vieta quindi una tale raccolta di dati personali e prevede la registrazione e la memorizzazione soltanto dei dati oggettivamente necessari a un'autorità per l'esecuzione del proprio compito (DTF **125** II 473 consid. 4b). Tuttavia, questa limitazione comporta problemi pratici difficilmente risolvibili: i dati in questione sono collegati tra loro dal punto di vista tecnico oppure la loro registrazione è necessaria per motivi tecnici. Inoltre, l'infrastruttura elettronica è in continua evoluzione, ragione per cui una definizione dettagliata e circoscritta delle registrazioni possibili diventerebbe necessariamente lacunosa dopo poco tempo. Infine, un elenco dettagliato sposterebbe l'accento (in termini di contenuti e di struttura) sulle disposizioni in materia di protezione dei dati, che occuperebbero uno spazio sproporzionato all'interno della LOGA. La limitazione viene attuata nella fase di trattamento successiva, non (ancora) in riferimento a persone, consentita soltanto per le finalità elencate in maniera esaustiva. Per l'ulteriore trattamento allo scopo di risalire a determinate persone è necessario soddisfare condizioni aggiuntive. In tal modo, la quantità di dati elaborata diminuisce con l'aumento delle condizioni e dell'intensità del trattamento.

La definizione di «infrastruttura elettronica» è volutamente generale, per evitare di doverla sempre adattare nel caso di innovazioni tecniche.

Abbiamo rinunciato a inserire un obbligo di emanare regolamenti per l'utilizzazione dell'infrastruttura elettronica della Confederazione. Tali regolamenti competono ai singoli

---

<sup>1</sup> A partire dall'1.1.2009 tale disposizione corrisponderà all'art. 57h; cfr. FF **2008** 1987

Dipartimenti; pur essendo senz'altro opportuna una loro armonizzazione, a nostro avviso non è necessaria alcuna disposizione legale apposita, ma piuttosto, per esempio, la redazione di regolamenti modello.

In diversi settori vengono applicate disposizioni speciali sul trattamento dei dati (p. es. legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, LSCPT; RS 780.1; Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna, LMSI; RS 120). Quanto sancito in queste leggi speciali prevale sulle disposizioni generali qui proposte.

## 2 Spiegazioni relative alle singole disposizioni

### Osservazione preliminare in merito all'attuale articolo 57a<sup>2</sup>

Questa disposizione introdotta nel 2000 rappresenta la base legale per il trattamento di dati personali degni di particolare protezione da parte di organi federali per mezzo di sistemi d'informazione e di documentazione per la registrazione, la gestione, l'indicizzazione e il controllo della corrispondenza e degli affari. Questa base legale si applica a gran parte dei settori dell'Amministrazione e ne copre numerose attività, come per esempio la gestione di un sistema elettronico di registrazione degli affari in corso oppure il trattamento e l'evasione delle richieste elettroniche.

Le disposizioni presentate qui di seguito sono intese a colmare le attuali lacune nell'ambito del trattamento elettronico dei dati. Riguardano anzitutto i cosiddetti dati marginali, ma in parte anche i contenuti di comunicazioni (p. es. oggetto e testo di una e-mail, contenuto di documenti Word).

### Articolo 57i Principi

I destinatari della nuova disposizione sono gli organi federali in qualità di gestori dell'infrastruttura elettronica, che possono registrare e trattare i dati generati da tale infrastruttura.

La revisione è volta alla protezione delle persone che utilizzano l'infrastruttura elettronica messa a disposizione dagli organi federali, ovvero in particolare il personale federale e i parlamentari.

*Capoverso 1:* è possibile registrare tutti i dati personali risultanti dall'utilizzazione dell'infrastruttura elettronica (quindi anche i contenuti di comunicazioni e video).

I *destinatari* delle disposizioni sono gli «organi federali», in altre parole gli stessi dell'attuale articolo 57a LOGA concernente il trattamento dei dati nell'ambito della gestione degli affari. Questo termine figura anche nella LPD (art. 2 cpv. 1 lett. b, art. 3 lett. h). Il concetto di organo federale è più ampio rispetto alle «unità amministrative» di cui all'articolo 2 LOGA e all'articolo 6 dell'ordinanza del 25 novembre 1998 sull'organizzazione del Governo e dell'Amministrazione (OLOGA; RS 172.010.1). Sono definiti organi federali:

- le autorità e i servizi della Confederazione (dipartimenti, uffici, Cancelleria federale, unità amministrative decentralizzate, istituti federali ecc.);
- le persone fisiche e giuridiche esterne all'Amministrazione federale cui sono affidati compiti federali (per es. Posta, FFS, Suva, PUBBLICA, SRG SSR idée suisse).

---

<sup>2</sup> A partire dall'1.1.2009 tale disposizione corrisponderà all'art. 57h; cfr. FF **2008** 1987

Questo implica che sono compresi anche l'Assemblea federale con i rispettivi organi, i Servizi del Parlamento per le proprie attività amministrative e le casse malati (cfr. a questo proposito Urs Maurer-Lambrou/Simon Kunz, «Kommentar zum DSG», in U. Maurer-Lambrou/Vogt: *Datenschutzgesetz – Basler Kommentar*, Basilea/Ginevra/Monaco 2006, art. 2 n. marg. 12 segg., Thomas Sägger, *Stämpflis Handkommentar zum RVOG*, art. 2 n. marg. 16 segg.). Le regole fissate per gli organi federali valgono anche per i servizi informatici che gestiscono l'infrastruttura su incarico di un organo federale.

Il presente avamprogetto parte dal presupposto che in linea di principio possono essere registrati *tutti* i dati personali generati dall'utilizzazione dell'infrastruttura elettronica della Confederazione, compresi per esempio i dati concernenti l'attivazione e la disattivazione di collegamenti elettronici tramite telefono o computer, nonché le registrazioni del tempo di lavoro del personale effettuate con gli appositi dispositivi. A un primo sguardo, la possibilità di registrare tutti i dati potrebbe risultare un'esagerazione. Tuttavia, separare i dati per cui è ammesso il trattamento successivo da quelli restanti, tecnicamente non è possibile oppure comporterebbe troppe imprecisioni (p. es. il computer non riesce a distinguere le e-mail private da quelle di lavoro). Inoltre, *de facto* le singole quantità di dati potrebbero essere specificate soltanto a titolo di esempio in un atto normativo. Per questo motivo, in virtù della protezione dei dati, il rispettivo trattamento viene limitato introducendo un elenco esaustivo degli scopi consentiti (art. 57k).

Le norme qui proposte vanno considerate come *lex generalis*, su cui hanno precedenza le disposizioni di leggi speciali.

Il *capoverso 2* contempla la prima limitazione: il trattamento dei dati registrati è ammesso soltanto per le finalità menzionate all'articolo 57k.

Il *capoverso 3* contiene una definizione più dettagliata dell'espressione «dati personali» (analogamente all'attuale art. 57a); è stabilito esplicitamente che le registrazioni possono contenere anche dati degni di particolare protezione e profili della personalità.

Il *capoverso 4* fa riferimento a un caso particolare disciplinato da una *lex specialis*: alla registrazione delle conversazioni telefoniche si applicano le condizioni rigide previste dagli articoli 179<sup>bis</sup> segg. del Codice penale (CP; RS 311.0).

## **Articolo 57j Infrastruttura elettronica**

L'infrastruttura riportata permette un'ampia interpretazione ed è volutamente definita in maniera generale, per evitare continui adeguamenti delle basi legali in risposta al progresso tecnologico. In linea di principio vanno citati tutti gli strumenti di lavoro, di ausilio e di controllo che gli organi federali mettono a disposizione dei loro impiegati ed eventualmente di terzi. Gli apparecchi in questione possono essere fissi o portatili.

## **Articolo 57k Finalità consentite per il trattamento dei dati**

*Capoverso 1*: i dati registrati possono essere trattati esclusivamente per le finalità riportate in questa disposizione. In questo ambito è possibile anche una combinazione di diverse finalità (p. es. confronto dei dati di controllo dei tempi di lavoro di una determinata persona con quelli sull'accesso della stessa a una collezione di dati). Per «trattamento» dei dati s'intende in linea di principio ogni ulteriore forma di elaborazione conforme alla LPD, dopo la registrazione secondo l'articolo 57i. La conservazione e la cancellazione dei dati, come forma particolare di trattamento, sono precisate nell'ordinanza (secondo l'art. 57l lett. a).

La lettera a fornisce una base legale per il salvataggio dati (copie di riserva), imprescindibile

e attualmente già praticato.

Inoltre, i dati devono poter essere analizzati a fini statistici (lett. b).

La lettera c ammette, tra gli altri, il trattamento dei dati concernenti l'attivazione e la disattivazione di collegamenti elettronici, nei seguenti casi:

- la manutenzione del sistema richiede in alcuni casi il trattamento dei dati per garantire la sicurezza delle informazioni e dei servizi (lett. c n. 1 e 2);
- per il controllo generale del rispetto dei regolamenti di utilizzazione (p. es. collegamenti a Internet non autorizzati) il fatto può essere chiarito, ma senza riferimenti a persone (lett. c n. 3);
- sulla base dei dati ottenuti deve essere possibile verificare da quale computer è stata consultata una determinata banca dati in quale momento, se sono state effettuate modifiche e quali (lett. c n. 4);
- deve inoltre essere possibile rilevare l'utilizzazione dell'infrastruttura elettronica, per esempio per addebitare i costi ai beneficiari dei servizi o per allestire statistiche (lett. c n. 5).

La lettera d permette per esempio la compilazione di dati in vista di modifiche degli orari di presenza obbligatori o di provvedimenti per la gestione della salute, nonché a fini statistici.

La lettera e ammette la classificazione di dati concernenti la sorveglianza video, per esempio in base a determinate fasce orarie.

*Capoverso 2:* sotto il profilo della protezione dei dati, il trattamento in riferimento a persone (analisi di dati per trarre deduzioni sul comportamento di una determinata persona) è una questione particolarmente delicata. Pertanto è ammesso soltanto nei casi previsti dalla legge. La lettera a ammette un tale trattamento dei dati se nel caso concreto sussiste un sospetto di utilizzazione abusiva dell'infrastruttura elettronica da parte di una determinata persona; non sono invece ammessi il trattamento in riferimento a persone per campioni o le analisi sistematiche. La lettera b ammette per esempio l'analisi in riferimento a determinate persone se è necessaria per l'individuazione di cause di guasti. La lettera c garantisce ad esempio l'analisi mensile dei dati riguardanti i tempi di lavoro, che permette al superiore di controllare le ore di lavoro straordinarie fornite dai propri collaboratori. La lettera d ammette la compilazione di dati in riferimento a una determinata persona per fatturarle i costi relativi all'utilizzo dell'infrastruttura elettronica soggetto a emolumento.

Al *capoverso 3* è fatto salvo il trattamento dei dati per scopi diversi, se ciò è previsto in un altro atto normativo. L'articolo 17 LPD descrive le esigenze che tali atti normativi devono adempiere. I dati possono essere trattati soltanto se sono rispettate le condizioni previste dalla legislazione speciale pertinente. Le situazioni regolamentate da tali atti normativi sono ad esempio i procedimenti penali (p. es. sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni sulla base della LSCPT; cfr. anche l'art. 246 segg. del nuovo Codice di procedura penale; FF 2007 6327), la sorveglianza video secondo la LMSI e l'art. 15 dell'ordinanza del 27 giugno 2001 sui servizi di sicurezza di competenza federale (OSF; RS 120.72), oppure il trattamento dei dati tramite sistemi d'informazione di polizia della Confederazione (cfr. il disegno di legge federale approvato dal Parlamento il 13.06.2008 sui sistemi d'informazione di polizia della Confederazione, LSIP; FF 2006 4661). Inoltre, anche la legge del 30 aprile 1997 sulle telecomunicazioni prevede disposizioni speciali (LTC; RS 784.10, art. 43-46).

## **Articolo 57/ Disposizioni d'esecuzione**

È anzitutto necessario sottolineare che la regolamentazione prevista si applica soprattutto a dati personali, facenti parte di quantità di dati in alcuni casi molto elevate; prima del trattamento effettivo, tali dati devono essere preparati adeguatamente (p. es. i collegamenti a Internet di una determinata persona devono essere isolati da tutti gli altri collegamenti, operazione che in alcuni casi è molto dispendiosa).

Le modalità di trattamento dei dati dopo la loro registrazione necessitano di un disciplinamento preciso. Tuttavia, nella legge è sufficiente un riferimento alle questioni principali che dovranno poi essere regolamentate nella rispettiva ordinanza. Il Consiglio federale deve quindi designare in particolare gli organi autorizzati e competenti per la registrazione e la conservazione dei dati. Deve inoltre disciplinare la durata di conservazione dei dati e la loro distruzione (lett. a). Deve anche specificare le modalità dell'ulteriore trattamento dei dati (lett. b). Infine, deve disciplinare come e quando un organo è autorizzato ad accedere e ad analizzare i dati (lett. c).

La regolamentazione proposta non riguarda un settore specifico, bensì numerosi casi diversi, motivo per cui un disciplinamento nella LOGA assumerebbe dimensioni sproporzionate a scapito della chiarezza. Per questo si rinuncia a una regolamentazione dettagliata delle modalità di trattamento dei dati nella legge, contrariamente a quanto avviene in settori più strutturati e chiaramente delimitati, come per esempio nel caso del disciplinamento previsto per il trattamento degli atti del personale nella LPers.

### **Modifica del diritto in vigore**

La regolamentazione prevista per gli organi federali deve valere anche per i tribunali federali, nella misura in cui è applicabile la LPD ed è interessata l'attività amministrativa. Visto che la LOGA non è applicabile ai tribunali, nelle tre leggi specifiche sui tribunali è necessario inserire un articolo che sancisca l'applicabilità delle nuove disposizioni sulla protezione dei dati secondo la LOGA.

Per i tribunali l'esecuzione non compete al Consiglio federale, bensì ai tribunali stessi, che devono quindi emanare le pertinenti disposizioni d'esecuzione necessarie.